The Open University

A second level
interdisciplinary
course

Exploring *Mathematics*

Groups

CHAPTER

D3

The Open University

A second level interdisciplinary course

Exploring *Mathematics*

BLOCK D
STRUCTURE IN MATHEMATICS

Groups

CHAPTER

D3

Prepared by the course team

About this course

This course, MS221 *Exploring Mathematics*, and the courses MU120 *Open Mathematics* and MST121 *Using Mathematics* provide a flexible means of entry to university-level mathematics. Further details may be obtained from the address below.

MS221 uses the software program Mathcad (MathSoft, Inc.) to investigate mathematical concepts and as a tool in problem solving. This software is provided as part of the course.

Contents

Study guide

This chapter is best studied in three sessions, although you may wish to divide your study of Section 2 into two parts.

> Study session 1: Subsections 1.1 and 1.2.
> Study session 2: Section 2.
> Study session 3: Section 3.

You should expect session 2 to take significantly longer than sessions 1 and 3. Note that Subsection 1.3 and Section 4 will not be assessed.

The optional computing work in Subsection 1.3 can be studied at any time after you have completed Subsections 1.1 and 1.2, or not at all. It describes techniques for using Mathcad to plot symmetric plane sets. Otherwise, the sections need to be studied in their printed order, and do not involve the use of any media other than print.

This chapter contains some material that is at a higher level of abstraction than you have encountered so far in the course. In Sections 2 and 3, in particular, you may find some of the material rather dense, and quite time-consuming to study.

1.1, 1.2

1.3

2

3

4
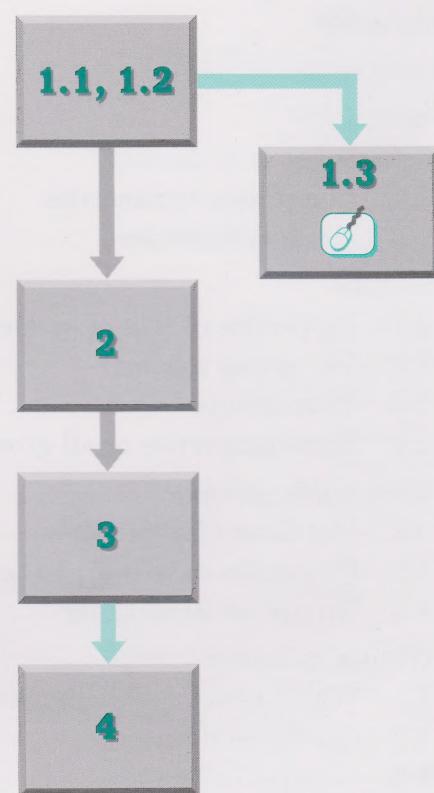
Introduction

The previous chapter discussed *number theory*. If you ask the question 'Why do we need numbers?', then you may receive answers such as 'Numbers are the 'tools' needed to do sums.'. Further thought leads to the conclusion that the fundamental purpose of numbers is to measure the *sizes* of various aspects of objects or phenomena, and to enable comparisons and relationships to be established between them. The sums that we learn to do with numbers are just techniques needed for this measuring and comparison.

However, when measuring and comparing objects, it is not only size that matters; the comparative structures, or patterns, of the objects may also be relevant. For example, in chemistry the same collection of atoms may combine in different ways to produce different molecules. The mathematical concept of a *group* was invented in the 19th century in order to classify the structures of certain objects, but it has proved since then to be fundamental to many other classification problems.

The definition of a group is rather abstract; indeed, a panel of experts at Princeton University decided in 1910 that group theory was 'useless'. However, it is precisely this abstractness, or generality, which makes group theory the appropriate language for discussing structure in subjects as diverse as the theory of equations, crystallography, geometry, particle physics, knot theory, bell-ringing and statistical data analysis.

See P.J. Davies and R. Hersh, *The Mathematical Experience*, Pelican, 1983.

In Chapters D1 and D2 we noted that the operations of addition and multiplication on real numbers have certain properties that are often, though not always, shared by other operations, such as addition and multiplication on complex numbers and on $\mathbb{Z}_n$. A group is a set with an operation that shares some of the properties of, say, addition of real numbers. However, we do not assume that the group operation has *all* the properties characteristic of addition on $\mathbb{R}$. The aim is to find a *generalisation* that retains enough of the properties of addition to be useful, but focuses on properties shared by a number of operations, so that results about groups are applicable in a wide variety of contexts. We assume that the group operation (say $*$) has two key properties. Firstly, it is associative; that is, $a * (b * c) = (a * b) * c$. Secondly, we want to be able to find an *inverse* for any group element. The idea of inverse generalises, for addition on $\mathbb{R}$, the negative of a real number, or, for multiplication on $\mathbb{R}$, the reciprocal of a real number. These assumptions enable us to use *some* of the manipulations of ordinary arithmetic when handling group elements.

Section 1 is devoted to the study of sets of symmetries in $\mathbb{R}^2$. In Section 2, we define the general concept of a group, and see many other examples of groups. We notice that certain groups, though arising in quite different contexts, show detailed similarities in their structure. In Section 3, we investigate the idea of two groups being 'essentially the same'. Finally, in the optional reading in Section 4, we give some brief indications of how groups have been used in a variety of different situations.

1   Symmetry

1.1   What is symmetry?

The natural world contains many objects which are symmetric. For example, evolution has created many animals with *bilateral*, that is, reflectional, symmetry, in which the left side of the animal appears to be the mirror image of the right side. This symmetry has been copied in objects as diverse as chairs, vehicles and buildings.

An object can be symmetric in many different ways, as exemplified in Figure 1.1. Each part of the figure represents a **plane set**; that is, a subset of $\mathbb{R}^2$.

(a)　　　　　　　　　(b)　　　　　　　　　(c)

(d)　　　　　　　　　(e)
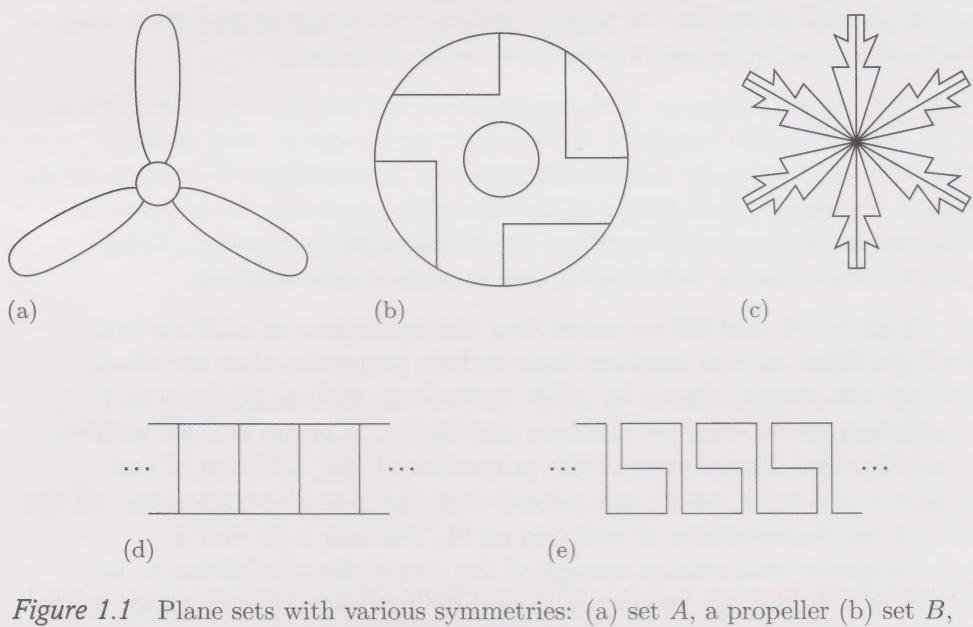
Figure 1.1   Plane sets with various symmetries: (a) set A, a propeller (b) set B, a wheel trim (c) set C, a snowflake (d) set D, a ladder (e) set E, a frieze

The ladder in Figure 1.1(d) and the frieze in (e) are assumed to extend indefinitely far both to the left and to the right, with the pattern repeating in each case. The five plane sets in Figure 1.1 can all be described as 'symmetric', but the nature of their symmetry is different in each case. For example, all the sets have rotational symmetry, but only three of them have any reflectional symmetry. Before looking at these examples in more detail, we need to make precise the meaning of this word 'symmetry'.

Roughly speaking, a *symmetry* of an object (or set) is an operation (or transformation) which leaves the object as a whole unchanged when it is applied. For example, in the case of bilateral symmetry, the appropriate operation is reflection in a mirror (or axis) through the middle of the object (Figure 1.2).

When dealing with plane sets the operations which we shall consider are the plane transformations called **isometries**. These are functions f from $\mathbb{R}^2$ to $\mathbb{R}^2$ which have the property that they preserve the distances between points; that is, for all P, Q in $\mathbb{R}^2$,

the distance from $f(P)$ to $f(Q)$ = the distance from P to Q.

Figure 1.2   A set symmetric about the vertical axis

From the Greek: isos meaning same, and metron meaning measure.

This distance-preserving property implies that an isometry must transform any given set to a set to which it is congruent.

There are four different types of isometries of $\mathbb{R}^2$; these are illustrated in Figures 1.3–1.6.
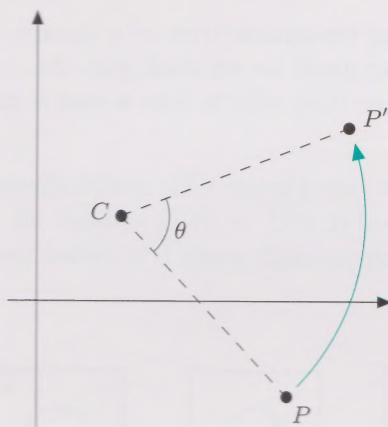
Figure 1.3   Rotation anticlockwise through angle θ about centre point C
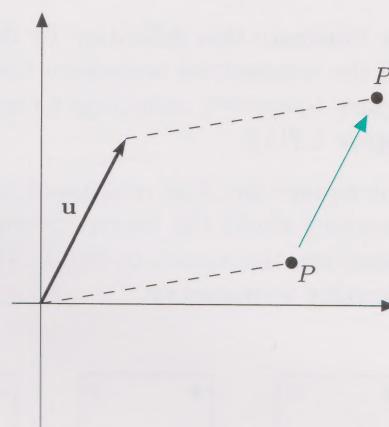
Figure 1.4   Translation by vector **u**
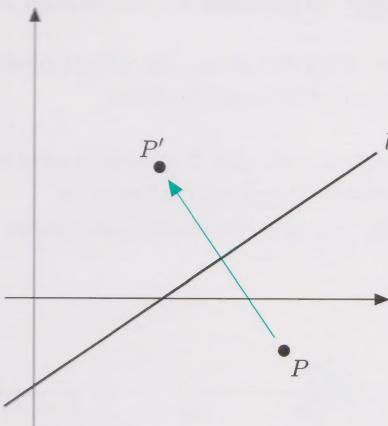
Figure 1.5   Reflection in line l, called the *axis of reflection*
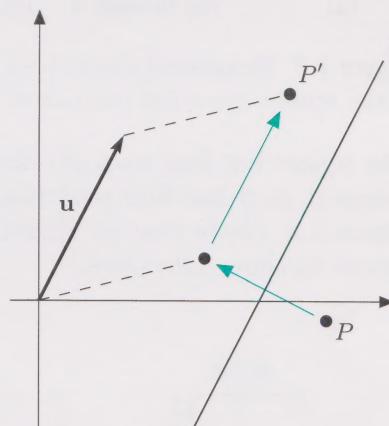
Figure 1.6   Glide-reflection in line l by vector **u** parallel to l

Notice that the **identity transformation**, which leaves every point invariant, can be seen as a rotation through angle 0, and also as a translation by the vector **0**. Also notice that two rotations about the same point C are identical, that is, they have the same effect, if their angles differ by an integer multiple of 2π.

Rotations and translations can both be carried out physically by making rigid movements within the plane. Reflections and glide-reflections, on the other hand, can only be carried out by moving outside the plane.

We are now ready to define the notion of a *symmetry* of a set, which might be thought of as an 'invisible isometry', since it appears to have no effect on the set as a whole.

Definition

A **symmetry** of a plane set X is a (plane) isometry which maps the set X to itself.

For example, reflection in the x-axis has the same effect on the x-axis as does the identity transformation.

Some texts insist that a symmetry of a set X should have domain X rather than $\mathbb{R}^2$. It is possible for two different plane isometries to have the same effect on each point of a set X, and so define the same symmetry, but this occurs rarely and we shall overlook the distinction to keep the above definition simple.

We illustrate this definition by determining the symmetries of a square. All the symmetries transform the square to itself, so we shall give the square *temporary* markings to help visualise their effects (the ● and ○ in Figure 1.7(a)).

It may help to construct your own model square. To see the effect of reflections, you will need to add the temporary markings on *both faces* of the square.

The square has four rotational symmetries (see Figure 1.7): anticlockwise rotations about the centre through angles of 0, $\pi/2$, π, $3\pi/2$ radians all transform the square to itself. The rotation through angle 0 is called the **identity symmetry**.

| (a) | (b) through 0 | (c) through $\pi/2$ | (d) through π | (e) through $3\pi/2$ |
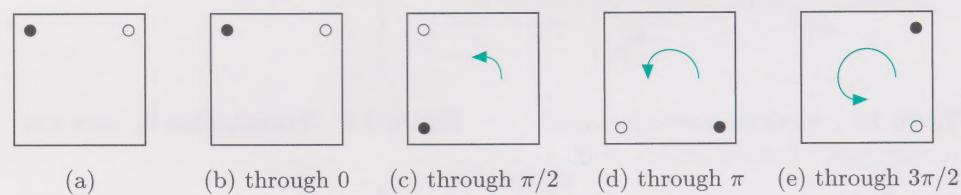
Figure 1.7   Rotational symmetries of a square. Part (a) shows the initial position of the square, the other parts show its position after various rotations

The square has four axes of reflection: one vertical, one horizontal and two diagonal, so it has four reflectional symmetries. These are shown in Figure 1.8. (Note that we shall consistently use double ended arrows in figures to show reflections.)

| (a) | (b) vertical axis | (c) horizontal axis | (d) diagonal axis | (e) other diagonal axis |
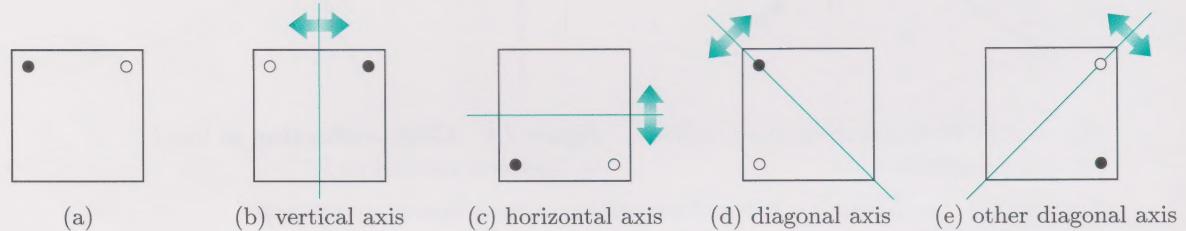
Figure 1.8   Reflectional symmetries of a square. Part (a) shows the initial position of the square, and the other parts show its position after various reflections

These appear to be *all* the symmetries of the square, but how can we be sure of this? One way is to observe that there are four possible corners for the ○ to move to, and after that two possible corners for the ●, making $4 \times 2 = 8$ possible symmetries altogether.

Thus the square has exactly eight symmetries, as shown in Figure 1.7(b)–(e) and Figure 1.8(b)–(e), the identity (trivial rotation), three non-trivial rotations, and four reflections.

Activity 1.1   Finding symmetries

Here we are concerned with identifying the symmetries of some of the sets shown in Figure 1.1.

(a) Consider set A, the propeller in Figure 1.1(a). Figure 1.9 shows this with temporary markings (● and ○), which we can use to help find symmetries.

   (i) To how many places can ○ move in a symmetry? For each possible image for ○, to how many places can ● move? How many symmetries does set A have in total?

   (ii) How many rotational symmetries does set A have? How many reflectional symmetries does it have? Do these give the correct total number of symmetries?

(b) Identify all the symmetries of set B, the wheel trim (see Figure 1.1(b)).

(c) What types of symmetries does set C, the snowflake (Figure 1.1(c)), have? How many of each are there?

Solutions are given on page 51.
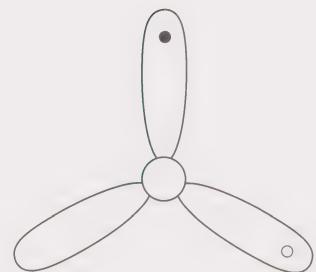
Figure 1.9   Set A, the propeller

Next, consider set D, the ladder (Figure 1.1(d)). This set has translational symmetries, as well as rotations and reflections. Indeed, it has infinitely many translational symmetries, some of which are represented by horizontal arrows in Figure 1.10. This diagram also shows a reflection in the horizontal axis down the middle of the ladder.
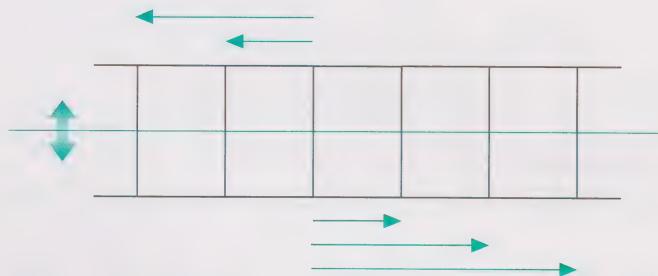
Figure 1.10   Some symmetries of set D, the ladder (from Figure 1.1(d))

Composing two of the symmetries shown in Figure 1.10, we see that the symmetries of the ladder also include glide-reflections such as that indicated in Figure 1.11.

(a)   (b)
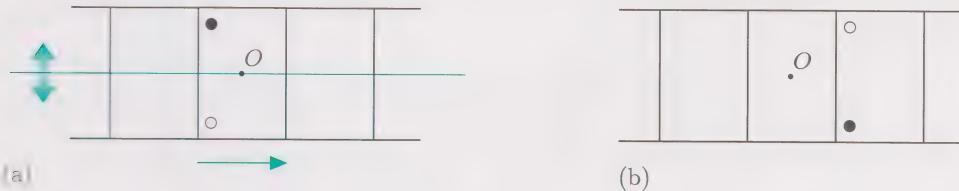
Figure 1.11   A glide-reflection that is a symmetry of set D. Part (a) shows the position of the ladder before, and (b) the position after, the transformation

9

The ladder also has infinitely many rotational symmetries, of two types, and infinitely many reflectional symmetries of two types. An example of each type is given in Figure 1.12.
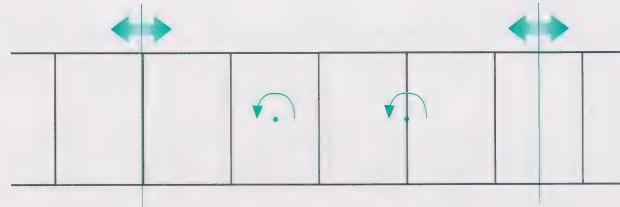
Figure 1.12   Rotational and reflectional symmetries of set D

Activity 1.2   Symmetries of the frieze

Describe the symmetries of set E, the frieze (Figure 1.1(e)).

Comment

The frieze has infinitely many translational symmetries in the horizontal direction (some examples are shown in Figure 1.13). It also has infinitely many of each of two types of rotation, as illustrated in Figure 1.13.
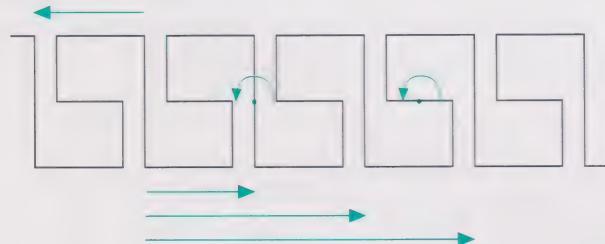
Figure 1.13   Symmetries of set E (from Figure 1.1(e))

The fact that the ladder and the frieze both have infinitely many symmetries may lead you to think that this has something to do with the fact that they are unbounded sets, whereas A, B and C are bounded sets. However, a disc has infinitely many rotational and reflectional symmetries (see Figure 1.14) and yet it is certainly a bounded set.

A **bounded** set in $\mathbb{R}^2$ is one which lies entirely inside some circle. An **unbounded** set is one that is not bounded.
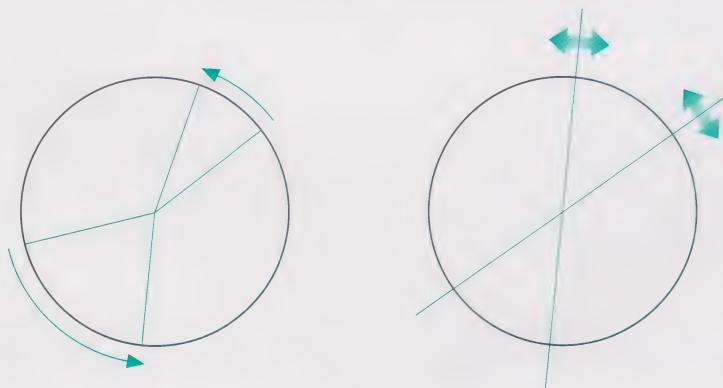
Figure 1.14   Examples of rotational and reflectional symmetries of a disc (Any rotation about its centre is a symmetry of the disc, as is any reflection in an axis through its centre)

Alternatively, an unbounded set may have only finitely many symmetries. For example, the graph $y = x^2$ (see Figure 1.15(a)) has just two symmetries (the identity symmetry and reflection in the y-axis), and the graph $y = x^4 - x^3$ (see Figure 1.15(b)) has just one (the identity symmetry).

(a)   (b)
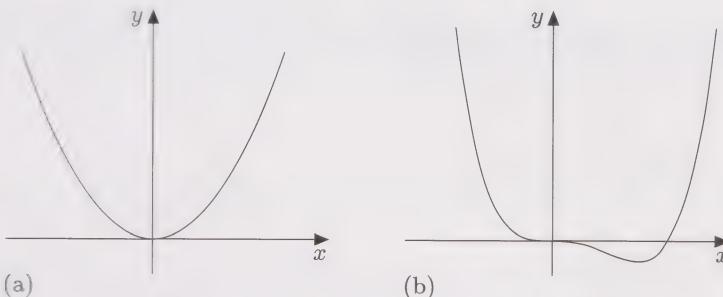
Figure 1.15 Two graphs: (a) $y = x^2$; (b) $y = x^4 - x^3$

It is true, however, that the sets of symmetries of unbounded sets are potentially much more complicated than those of bounded sets. For example, all symmetries of a bounded set must be either rotations or reflections. (This is because the presence of a *single* non-trivial translation or glide-reflection would imply the presence of infinitely many of these, with displacements given by arbitrarily long vectors.)

In this chapter we shall focus mainly on the symmetries of bounded sets, and so we work almost exclusively with rotations and reflections. Wherever possible, we place such bounded sets with their centres at the origin, and then we need to consider only rotations and reflections of two special types, denoted by r_θ and q_ϕ, where:

This notation was introduced in Chapter A3, Section 2.

r_θ is a rotation anticlockwise about O through an angle θ, $0 \le \theta < 2\pi$ (see Figure 1.16);

q_ϕ is a reflection in an axis through O at an angle ϕ to the positive x-axis, $0 \le \phi < \pi$ (see Figure 1.17).
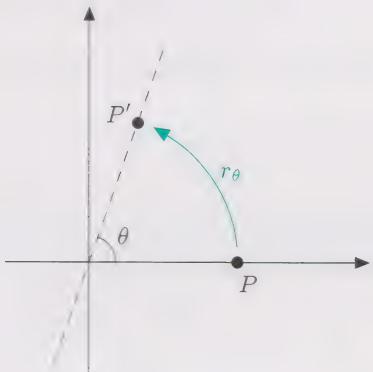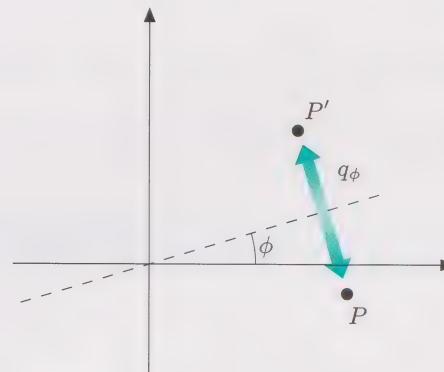
Figure 1.16 r_θ *Figure 1.17* q_ϕ

The condition $0 \le \theta < 2\pi$ ensures that each rotation about O is included exactly once. The rotation r_0 is the identity symmetry of any plane set, usually called e. (This notation derives from the German word 'einheit', which means unity.) Similarly, the restriction $0 \le \phi < \pi$ ensures that each reflection in an axis through O is included exactly once. Notice that q_0 denotes reflection in the x-axis and is *not* the same as e.

11

Figure 1.18   The images of $(1,1)$ under r_π and q_0

We should emphasise that r_θ and q_ϕ are names of *functions* (the corresponding isometries of the plane), so we can write equations such as

$$q_0(1,1) = (1,-1) \quad \text{and} \quad r_\pi(1,1) = (-1,-1),$$

to denote function evaluations (see Figure 1.18).

Activity 1.3   Function evaluations

Evaluate: (a) $r_{\pi/2}(1,1)$;   (b) $q_{\pi/2}(1,1)$;   (c) $q_{\pi/4}(2,0)$;   (d) $r_{\pi/4}(1,0)$.

Solutions are given on page 51.

Using the r_θ, q_ϕ notation, we can represent the symmetries of a square centred at the origin, and with sides parallel to the axes. Since we shall often consider the set of symmetries of this square, we give it the special name $S(\square)$. Thus, as illustrated in Figure 1.19,

$$S(\square) = \{e, r_{\pi/2}, r_\pi, r_{3\pi/2}, q_0, q_{\pi/4}, q_{\pi/2}, q_{3\pi/4}\}.$$

We take for granted the presence of the identity, e.
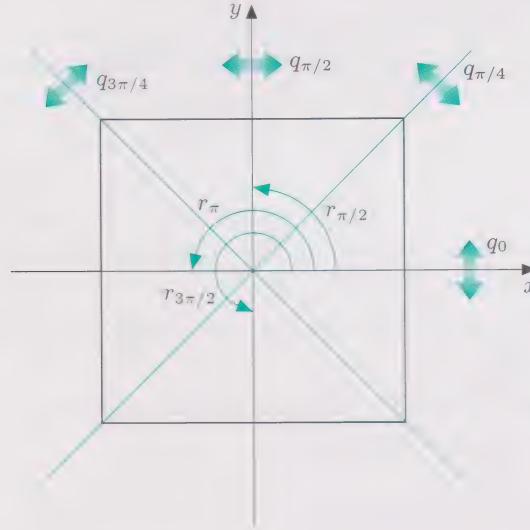
Figure 1.19   All the symmetries of a square (with sides parallel to the axes)

For a general set X we use the notation $S(X)$ to denote the set of symmetries of X.

Activity 1.4   Sets of symmetries

Let the sets A, B and C be as illustrated in Figure 1.1, and considered in Activity 1.1. Write down $S(A)$, $S(B)$ and $S(C)$, using the r_θ, q_ϕ notation. (Assume that the centres of A, B and C are at the origin of an (x,y) coordinate system.)

A solution is given on page 51.

The sets of symmetries of regular polygons have a major role to play in what follows. We have already determined $S(\square)$, and the set of symmetries of the propeller is the same as the set of symmetries of an equilateral triangle with its vertices at the tips of the propeller blades. We use the name $S(\triangle)$ for the set of symmetries of an equilateral triangle in this position, and these symmetries are shown in Figure 1.20. Note that

$$S(\triangle) = \{e, r_{2\pi/3}, r_{4\pi/3}, q_{\pi/6}, q_{\pi/2}, q_{5\pi/6}\}.$$

A *regular polygon* is one with equal sides and equal angles.
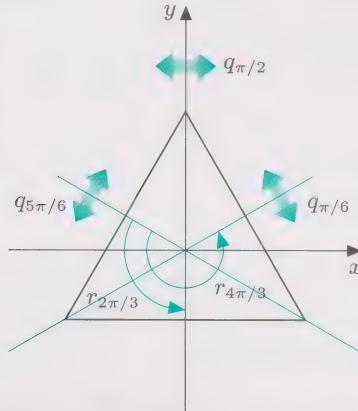
Figure 1.20   The symmetries of an equilateral triangle

More generally, a regular polygon with n sides, called an **n-gon**, has $2n$ symmetries:

◇ n rotations, through integer multiples of $2\pi/n$;

◇ n reflections, in axes of symmetry through the centre, the angle between adjacent axes being π/n.

It is standard practice to draw an n-gon with one edge as its horizontal base. Figure 1.21 shows the symmetries of regular n-gons with $n = 5$ (the regular pentagon) and $n = 6$ (the regular hexagon).

(a)   (b)

Note that the set of symmetries of the regular hexagon is identical to the set of symmetries of the snowflake, found in Activity 1.4.
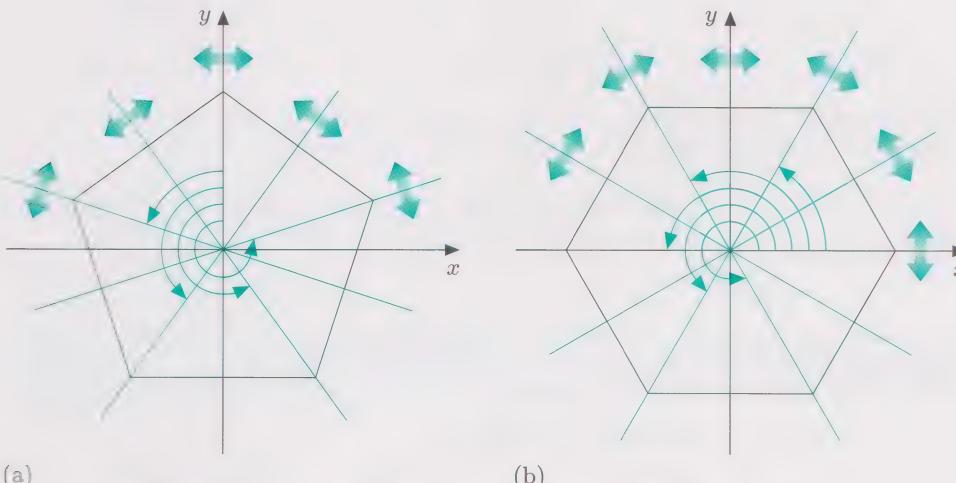
Figure 1.21   The symmetries of: (a) a regular pentagon; (b) a regular hexagon

We denote the sets of symmetries of a regular pentagon and of a regular hexagon (in standard position) by $S(\text{PENT})$ and $S(\text{HEX})$, respectively. We also denote by $S(\square)$ the set of symmetries of a (non-square) rectangle with its centre at O and its sides parallel to the axes.

Activity 1.5   Sets of symmetries of polygons

Use the r_θ, q_ϕ notation to write down all the symmetries in

(a) $S(\text{PENT})$,   (b) $S(\square)$.

Comment

(a) The symmetries in $S(\text{PENT})$ are shown in Figure 1.21(a). Notice that
the y-axis is one axis of reflection, corresponding to the symmetry $q_{\pi/2}$.
The other axes of reflection make angles with the y-axis that are
multiples of $\pi/5$. Rotational symmetries of the pentagon are through
angles of 0 (the identity), and through multiples of $2\pi/5$. So we have:

$$S(\text{PENT}) = \{e, r_{2\pi/5}, r_{4\pi/5}, r_{6\pi/5}, r_{8\pi/5}, q_{\pi/10}, q_{3\pi/10}, q_{\pi/2}, q_{7\pi/10}, q_{9\pi/10}\}.$$

(b) The non-trivial symmetries of a rectangle are shown in Figure 1.22.
We see that

$$S(\square) = \{e, r_\pi, q_0, q_{\pi/2}\}.$$

Figure 1.22

1.2   Composing symmetries

Since the symmetries of a set X are isometries which transform X onto
itself, we can form the composition of any two symmetries of X and obtain
another symmetry of X.

For example, consider the symmetries $r_{\pi/2}$ and q_0 of the square. Then
$q_0 \circ r_{\pi/2}$ denotes the symmetry obtained by performing *first* $r_{\pi/2}$ and *then*
q_0. One way to find which element of $S(\square)$ is equal to $q_0 \circ r_{\pi/2}$ is to mark
the square to watch the effect of $r_{\pi/2}$ followed by q_0; see Figure 1.23.
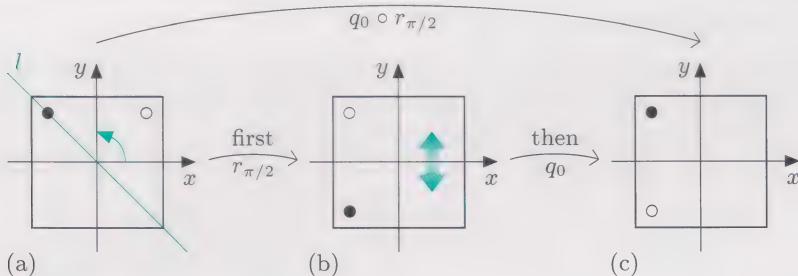
Figure 1.23   Starting as in (a), we first rotate through $\pi/2$, then reflect in the
x-axis. The combined effect is the same as that of reflection in the line l

Comparing the initial and final positions of the markings, we see that the
effect of $q_0 \circ r_{\pi/2}$ on the square is the same as the effect of $q_{3\pi/4}$. Thus

$$q_0 \circ r_{\pi/2} = q_{3\pi/4}.$$

Activity 1.6   Composing symmetries from $S(\square)$

Find the following composite symmetries.

(a) $r_{\pi/2} \circ r_\pi$ (b) $q_{\pi/4} \circ q_{\pi/4}$ (c) $r_{\pi/2} \circ q_0$ (d) $q_{\pi/4} \circ q_{3\pi/4}$

You should be able to find the answer to (a) and (b) by visualising the
effects of the successive symmetries. For (c) and (d), you may find it
helpful to consider the effect of the successive symmetries on a disc,
centred at the origin, and suitably marked with ● and ○.

Solutions are given on page 52.

It would take rather longer to determine the composites of all pairs of symmetries in $S(\square)$, in both possible orders. The result of this calculation is displayed in Table 1.1, below. Here a composite of the form $a \circ b$ is placed in the row labelled a and the column labelled b (you can use this table to check your answers to Activity 1.6). Such a table is called a **Cayley table**. Note that each border of the table contains all the members of the set

$$S(\square) = \{e, r_{\pi/2}, r_\pi, r_{3\pi/2}, q_0, q_{\pi/4}, q_{\pi/2}, q_{3\pi/4}\},$$

and that the members are arranged in the same order on both borders. Cayley tables are always arranged in such a way.

Arthur Cayley (1821–1895) was the leading British algebraist of the 19th century. He helped to lay the groundwork for group theory, and developed the algebra of matrices and determinants.

Table 1.1 A Cayley table for $S(\square)$

$\circ$	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
e	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
$r_{\pi/2}$	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	e	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0
r_π	r_π	$r_{3\pi/2}$	e	$r_{\pi/2}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0	$q_{\pi/4}$
$r_{3\pi/2}$	$r_{3\pi/2}$	e	$r_{\pi/2}$	r_π	$q_{3\pi/4}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$
q_0	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	e	$r_{3\pi/2}$	r_π	$r_{\pi/2}$
$q_{\pi/4}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$r_{\pi/2}$	e	$r_{3\pi/2}$	r_π
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	r_π	$r_{\pi/2}$	e	$r_{3\pi/2}$
$q_{3\pi/4}$	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$r_{3\pi/2}$	r_π	$r_{\pi/2}$	e

We have used tint to highlight some features of the table which are discussed below.

This table has several interesting features. First, it is not symmetric about the main diagonal; for example,

$$r_{\pi/2} \circ q_{\pi/2} = q_{3\pi/4} \quad \text{but} \quad q_{\pi/2} \circ r_{\pi/2} = q_{\pi/4}.$$

Each quarter of the table contains either 'all rotations' or 'all reflections'. This occurs because: two rotations produce a rotation, a rotation and reflection (in either order) produce a reflection, whereas two reflections produce a rotation. Finally, the top-left quarter has the 'constant diagonal' pattern seen in the addition table for $\mathbb{Z}_4$, in Table 1.2.

See Chapter D2, Section 3.

To see how Table 1.1 above may be drawn up, we now derive formulas which give the result of composing *any* pair of rotations or reflections.

First, consider the effect of composing two rotations: first r_θ then r_ϕ, where $0 \le \theta < 2\pi$ and $0 \le \phi < 2\pi$. The overall effect is the same as that of a rotation through $\phi + \theta$. Thus, if $\phi + \theta < 2\pi$, then we can write $r_\phi \circ r_\theta = r_{\phi+\theta}$. However, if $\phi + \theta \ge 2\pi$, then $r_\phi \circ r_\theta = r_{\phi+\theta-2\pi}$. If we perform these two rotations in the reverse order, first r_ϕ, then r_θ, the overall effect is the same, so we have $r_\theta \circ r_\phi = r_\phi \circ r_\theta$.

Table 1.2 Addition table for $\mathbb{Z}_4$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

To avoid having two formulas, we use a notation similar to that for modular arithmetic, by defining $\alpha \pmod{2\pi}$ to be the unique angle which:

   differs from α by a multiple of 2π;

   satisfies the condition $0 \le \alpha \pmod{2\pi} < 2\pi$.

Using this notation, we obtain the single formula

For example,

$$\frac{5\pi}{2} \pmod{2\pi} = \frac{\pi}{2}.$$

$$r_\phi \circ r_\theta = r_{\phi+\theta \pmod{2\pi}}.$$

It is a little trickier to find the composite $r_\phi \circ q_\theta$. Both r_ϕ and q_θ are symmetries of a disc centred at the origin, and so $r_\phi \circ q_\theta$ will be also. To find its effect, we use the technique of marking the disc with $\bullet$ and $\circ$. It is convenient to place $\bullet$ on the x-axis and $\circ$ on the axis of reflection of q_θ (see Figure 1.24).
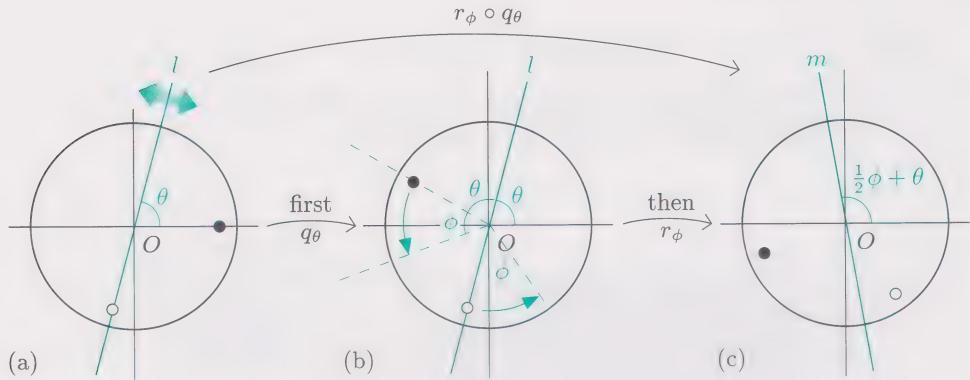
Figure 1.24 Starting as in (a), we first reflect in the line l, then rotate through ϕ

Comparing the initial and final positions of $\circ$, we see that it has been rotated about O through the angle ϕ, while comparison of the initial and final positions of $\bullet$ show that this has been rotated about O by a total angle of $\phi + 2\theta$. These effects on $\circ$ and $\bullet$ are the same as those of reflection in the line m shown in Figure 1.24(c), which is at an angle of $\frac{1}{2}\phi + \theta$ to the positive x-axis. Thus the overall effect of the composition $r_\phi \circ q_\theta$ is the same as that of $q_{\frac{1}{2}\phi+\theta}$. To be precise (since the angle $\frac{1}{2}\phi + \theta$ may exceed π), we adapt the modular arithmetic notation once again, and write:

$$r_\phi \circ q_\theta = q_{\frac{1}{2}\phi+\theta \,(\mathrm{mod}\ \pi)}.$$

A similar approach can be used to establish the other entries in the following summary table.

An alternative way to derive these results is to use the matrix representations of r_θ and q_θ, given in Chapter B2, Section 1, together with matrix multiplication.

Table 1.3 Composing rotations and reflections in $\mathbb{R}^2$

$\circ$	r_θ	q_θ
r_ϕ	$r_{\phi+\theta \,(\mathrm{mod}\ 2\pi)}$	$q_{\frac{1}{2}\phi+\theta \,(\mathrm{mod}\ \pi)}$
q_ϕ	$q_{\phi-\frac{1}{2}\theta \,(\mathrm{mod}\ \pi)}$	$r_{2\phi-2\theta \,(\mathrm{mod}\ 2\pi)}$

Activity 1.7 Compiling Cayley tables

(a) Use Table 1.3 to calculate each of the following.

    (i) $r_{4\pi/3} \circ r_{2\pi/3}$ (ii) $r_{2\pi/3} \circ q_{\pi/2}$

    (iii) $q_{\pi/2} \circ r_{4\pi/3}$ (iv) $q_{\pi/6} \circ q_{\pi/2}$

$S(\square)$ was shown in Figure 1.22 and $S(\triangle)$ in Figure 1.20.

(b) Construct a Cayley table for $S(\square) = \{e, r_\pi, q_0, q_{\pi/2}\}$.

(c) Construct a Cayley table for $S(\triangle) = \{e, r_{2\pi/3}, r_{4\pi/3}, q_{\pi/6}, q_{\pi/2}, q_{5\pi/6}\}$.

Comment

(a) (i) Using the upper-left entry in Table 1.3:

$$r_{4\pi/3} \circ r_{2\pi/3} = r_{4\pi/3+2\pi/3 \ (\text{mod } 2\pi)} = r_{6\pi/3 \ (\text{mod } 2\pi)} = r_0 = e.$$

(ii) Using the upper-right entry:

$$r_{2\pi/3} \circ q_{\pi/2} = q_{\pi/3+\pi/2 \ (\text{mod } \pi)} = q_{5\pi/6}.$$

(iii) Using the lower-left entry:

$$q_{\pi/2} \circ r_{4\pi/3} = q_{\pi/2-2\pi/3 \ (\text{mod } \pi)} = q_{-\pi/6 \ (\text{mod } \pi)} = q_{5\pi/6}.$$

(iv) Using the lower-right entry:

$$q_{\pi/6} \circ q_{\pi/2} = r_{\pi/3-\pi \ (\text{mod } 2\pi)} = r_{-2\pi/3 \ (\text{mod } 2\pi)} = r_{4\pi/3}.$$

(b) Since each symmetry of the rectangle is also a symmetry of the square, the Cayley table of $S(\square)$ can in fact be read off from the Cayley table of $S(\square)$. We obtain the table shown in the margin.

$\circ$	e	r_π	q_0	$q_{\pi/2}$
e	e	r_π	q_0	$q_{\pi/2}$
r_π	r_π	e	$q_{\pi/2}$	q_0
q_0	q_0	$q_{\pi/2}$	e	r_π
$q_{\pi/2}$	$q_{\pi/2}$	q_0	r_π	e

(c) The Cayley table is shown below. We calculated four of the entries in part (a), and the other entries are calculated in a similar way using Table 1.3. (We shall not discuss the details of this.)

$\circ$	e	$r_{2\pi/3}$	$r_{4\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$
e	e	$r_{2\pi/3}$	$r_{4\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$
$r_{2\pi/3}$	$r_{2\pi/3}$	$r_{4\pi/3}$	e	$q_{\pi/2}$	$q_{5\pi/6}$	$q_{\pi/6}$
$r_{4\pi/3}$	$r_{4\pi/3}$	e	$r_{2\pi/3}$	$q_{5\pi/6}$	$q_{\pi/6}$	$q_{\pi/2}$
$q_{\pi/6}$	$q_{\pi/6}$	$q_{5\pi/6}$	$q_{\pi/2}$	e	$r_{4\pi/3}$	$r_{2\pi/3}$
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/6}$	$q_{5\pi/6}$	$r_{2\pi/3}$	e	$r_{4\pi/3}$
$q_{5\pi/6}$	$q_{5\pi/6}$	$q_{\pi/2}$	$q_{\pi/6}$	$r_{4\pi/3}$	$r_{2\pi/3}$	e

---

Activity 1.8   Symmetries of the wheel trim

Draw up a Cayley table for the set of symmetries of the wheel trim (Figure 1.1(b)), which is

$$S(\text{TRIM}) = \{e, r_{\pi/2}, r_\pi, r_{3\pi/2}\}.$$

A solution is given on page 52.

1.3 Using symmetries

The Mathcad files associated with this chapter demonstrate how an understanding of the symmetries of a plane set, such as a snowflake, can facilitate the process of plotting the plane set with a computer package.

Refer to Computer Book D for the work in this subsection.

This subsection will not be assessed.

Summary of Section 1

Rotations, reflections, translations and glide-reflections form the isometries of the plane. For any particular set X in $\mathbb{R}^2$, those isometries that map X to itself are called symmetries of X. (We include the identity function, denoted by e, as a symmetry of any plane set.)

We identified the sets of symmetries of various plane sets. We were particularly concerned with bounded sets, centred at the origin, which can only have symmetries of the forms r_θ (rotation about O) and q_ϕ (reflection in a line through O).

The composites of the symmetries of a plane set can be shown in a Cayley table. For example, we gave a Cayley table for $S(\square)$, the set of symmetries of a square. In Table 1.3, we gave formulas for composing r_θ and q_ϕ.

Exercises for Section 1

Exercise 1.1

Use Table 1.3 to calculate each of (a)–(d).

(a) $q_{\pi/4} \circ q_{\pi/2}$ (b) $q_{\pi/2} \circ q_{\pi/4}$ (c) $r_{2\pi/3} \circ q_{\pi/4}$ (d) $q_{\pi/4} \circ r_{2\pi/3}$

Exercise 1.2

For each of the plane sets A, B and C shown in Figure 1.25, find the set of symmetries of the plane set and compile the corresponding Cayley table. The set A is an isosceles triangle, symmetric under reflection in the y-axis; the set B is an equilateral triangle with centre at the origin, one vertex on the y-axis, and some parts coloured; the set C is a rhombus with its vertices on the axes.

(a)   (b)   (c)
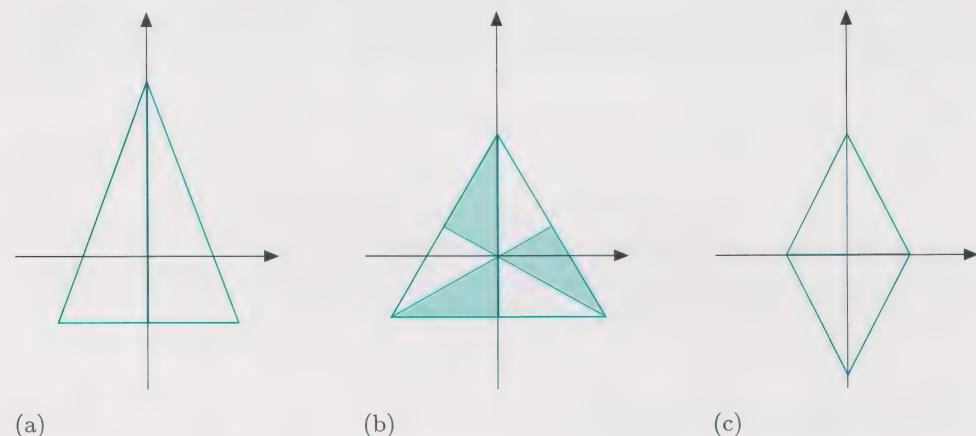
Figure 1.25   (a) Set A, (b) set B and (c) set C

2 Groups

In this section, we first highlight certain properties of the set of symmetries of any plane set. These properties are remarkably similar to some of the familiar properties of arithmetic, and this similarity leads us to define the abstract structure known as a *group*.

2.1 Properties of sets of symmetries

In Section 1 we found that the square has eight symmetries. These form the set $S(\square)$, and combine together under composition as shown in its Cayley table (Table 1.1, reproduced below).

$\circ$	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
e	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
$r_{\pi/2}$	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	e	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0
r_π	r_π	$r_{3\pi/2}$	e	$r_{\pi/2}$	$q_{\pi/2}$	$q_{3\pi/4}$	q_0	$q_{\pi/4}$
$r_{3\pi/2}$	$r_{3\pi/2}$	e	$r_{\pi/2}$	r_π	$q_{3\pi/4}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$
q_0	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	e	$r_{3\pi/2}$	r_π	$r_{\pi/2}$
$q_{\pi/4}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	$q_{\pi/2}$	$r_{\pi/2}$	e	$r_{3\pi/2}$	r_π
$q_{\pi/2}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$q_{3\pi/4}$	r_π	$r_{\pi/2}$	e	$r_{3\pi/2}$
$q_{3\pi/4}$	$q_{3\pi/4}$	$q_{\pi/2}$	$q_{\pi/4}$	q_0	$r_{3\pi/2}$	r_π	$r_{\pi/2}$	e

We shall use this Cayley table to illustrate certain key properties of the set of symmetries of *any* plane set. The first property, already noted in Section 1, is that any two symmetries of a plane set combine together under composition to produce another symmetry of that set. In relation to the Cayley table for $S(\square)$, this property means that all 64 entries in the body of the table are elements of $S(\square)$ itself. The word *closure* is used to describe this property, which we now state formally.

> **Property 1**
>
> The set of symmetries $S(X)$ of a plane set X is **closed** under the operation of composition; that is, for all $f, g \in S(X)$,
>
> $$g \circ f \in S(X).$$

Similarly, the set $\mathbb{R}$ of real numbers is closed under the operations of both addition and multiplication.

Another property which is evident in the Cayley table for $S(\square)$ is that the identity symmetry e has no effect on other symmetries when composed with them. The identity, e, is a symmetry of *any* plane set.

> **Property 2**
>
> The set of symmetries $S(X)$ of a plane set X contains the **identity** symmetry e with the property that, for all $f \in S(X)$,
>
> $$e \circ f = f = f \circ e.$$

Similarly, in $\mathbb{R}$ the number 0 is an identity for addition and 1 is an identity for multiplication.

The identity symmetry e appears in every row and every column of the Cayley table for $S(\square)$, and moreover its appearances are symmetric about the main diagonal of the table. This pattern occurs because each

symmetry f of a plane set X is an isometry, and any isometry is one-one, and so f has an inverse function f^{-1}. This inverse function must also be an isometry, and indeed must be a symmetry of X. Since

$$f^{-1} \circ f = e \quad \text{and} \quad f \circ f^{-1} = e,$$

the appearances of e in the Cayley table are symmetric.

Property 3

Each symmetry f in $S(X)$ has an **inverse** symmetry f^{-1} in $S(X)$ with the property that

$$f \circ f^{-1} = e = f^{-1} \circ f.$$

Similarly, for each x in $\mathbb{R}$,
$x + (-x) = 0 = (-x) + x$,
and, for each non-zero x in $\mathbb{R}$,
$x \times (1/x) = 1 = (1/x) \times x$.

We can read off the inverses of the symmetries in $S(\square)$ from the positions of the identity in the Cayley table.

For example, e appears at the intersection of the $r_{\pi/2}$ row and $r_{3\pi/2}$ column, and at the intersection of the $r_{3\pi/2}$ row and $r_{\pi/2}$ column.

symmetry	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$
inverse	e	$r_{3\pi/2}$	r_π	$r_{\pi/2}$	q_0	$q_{\pi/4}$	$q_{\pi/2}$	$q_{3\pi/4}$

Notice that each reflection is its own inverse, since if we perform a reflection twice every point is returned to its initial position. We say that reflections are **self-inverse**. The identity e is also self-inverse, as is the rotation r_π, but other rotations are not.

For $0 < \theta < 2\pi$, the isometry r_θ is a rotation anticlockwise about O through an angle θ, and its effect can be reversed by the corresponding *clockwise* rotation through θ. Since this rotation has the same effect as the rotation through an angle $2\pi - \theta$ anticlockwise about O, we can deduce the result about inverses of rotations given in part (b) of the following theorem.

Theorem 2.1   Inverses of Rotations and Reflections

(a) $e^{-1} = e$;

(b) $r_\theta^{-1} = r_{2\pi-\theta}$, for $0 < \theta < 2\pi$;

(c) $q_\phi^{-1} = q_\phi$. for $0 \leq \phi < \pi$.

The next activity gives you a chance to practise finding inverses.

Activity 2.1   Checking inverses

Use the Cayley table for $S(\triangle)$, found in Activity 1.7(c), to determine the inverse of each element of $S(\triangle)$. Check that these inverses satisfy Theorem 2.1.

A solution is given on page 52.

There is one further number-like property of any set of symmetries $S(X)$ which is not immediately apparent from the Cayley table of $S(X)$. Both addition and multiplication of numbers are *associative*; that is, for all real numbers x, y, z,

$$x + (y + z) = (x + y) + z \quad \text{and} \quad x \times (y \times z) = (x \times y) \times z.$$

It is associativity of addition that allows us to write sums of several terms without brackets, as in $a + b + c + d + x$, for example. Similarly, associativity of multiplication allows us to write products without brackets, such as $a \times b \times c \times d \times x$.

Now, if f, g and h are symmetries of a set X, then the functions

$$h \circ (g \circ f) \quad \text{and} \quad (h \circ g) \circ f$$

are symmetries of X, by Property 1. However, both these symmetries are achieved by performing

first f, then g and finally h,

and so $h \circ (g \circ f) = (h \circ g) \circ f$. Thus composition of symmetries is associative. This result arises from the fact that composition of functions is associative in general. For any functions f, g and h for which these compositions exist, we have, as illustrated in Figure 2.1,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$
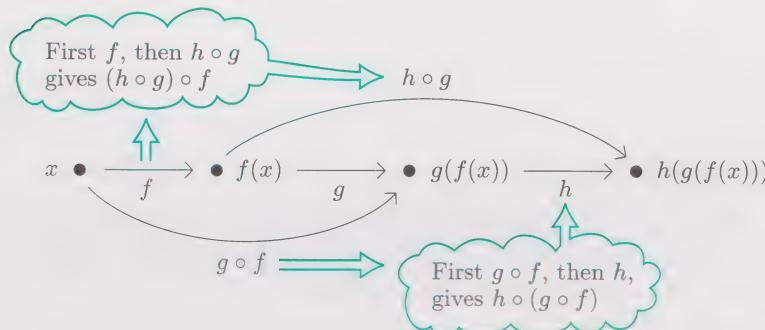
Figure 2.1   Composition of functions is associative: $h \circ (g \circ f) = (h \circ g) \circ f$

Property 4

Composition of symmetries is **associative**; that is, for all $f, g, h \in S(X)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Activity 2.2   Checking associativity

Use the Cayley table for $S(\square)$ to check that the following are equal:

$$r_{\pi/2} \circ (q_{\pi/4} \circ r_{3\pi/2}) \quad \text{and} \quad (r_{\pi/2} \circ q_{\pi/4}) \circ r_{3\pi/2}.$$

A solution is given on page 52.

2.2 The group axioms

It is a remarkable fact that many sets of elements have associated operations which satisfy the four properties of closure, identity, inverses and associativity. This makes it worthwhile to study all such sets simultaneously by introducing an abstract structure called a *group*. A group is a set, with an associated operation for combining pairs of elements of the set, which satisfies all *four* properties listed above. The technical name for an operation which combines pairs of elements of a set is a **binary operation**.

Definition

Let G be a set and $*$ a binary operation on G. Then $(G, *)$ is a **group** if the following four properties hold.

G1 **Closure** For all $g, h \in G$,

$$g * h \in G.$$

G2 **Identity** There exists an identity element $e \in G$ such that, for all $g \in G$,

$$g * e = g = e * g.$$

G3 **Inverses** For all $g \in G$, there exists an inverse element $g^{-1} \in G$, such that

$$g * g^{-1} = e = g^{-1} * g.$$

G4 **Associativity** For all $g, h, k \in G$,

$$g * (h * k) = (g * h) * k.$$

The concept of a group is extremely general. The set G may consist of elements such as: integers, real numbers, complex numbers, symmetries, real functions, or matrices; and the operation $*$ may be $+$, $\times$, $\circ$ or something quite different. For a *general* group, we usually use the notation in the definition: G for the set; $*$ for the operation; e for the identity; letters such as g, h, k, for the elements of G, and g^{-1} (etc) for inverses. However, for a specific group, with a particular set G and operation $*$, it may be appropriate to use a different notation. Also, instead of saying '$(G, *)$ is a group', we may say 'G is a group under the operation $*$'.

We sometimes refer to 'a group G', rather than to $(G, *)$, when the operation is evident or unimportant.

We refer to G1, G2, G3 and G4 as the *group axioms*. They are the fundamental assumptions which we make about a group, and all theorems about groups must be derived from them, using any other known properties of the group or groups being considered.

Because the four group axioms are just Properties 1, 2, 3 and 4 of $S(X)$, the following result has already been established, and it gives many examples of groups.

Theorem 2.2   Symmetry groups

The set $S(X)$ of symmetries of a plane set X forms a group under the operation $\circ$.

From now on, we shall call $S(X)$ the **symmetry group** of X.

However, there are many other types of groups, including groups of numbers which arise from the properties of arithmetic. For example, the set of integers $\mathbb{Z}$ forms a group under the operation $+$, as can easily be checked. We write this verification out in a formal way below.

G1 *Closure* For all $m, n \in \mathbb{Z}$,
$$m + n \in \mathbb{Z},$$
and so $\mathbb{Z}$ is closed under $+$.

G2 *Identity* The number $0 \in \mathbb{Z}$ and, for all $m \in \mathbb{Z}$,
$$m + 0 = m = 0 + m,$$
so 0 is an identity element.

G3 *Inverses* For all $m \in \mathbb{Z}$, there exists $-m \in \mathbb{Z}$ with
$$m + (-m) = 0 = (-m) + m,$$
so each element m has an inverse in $\mathbb{Z}$.

We call $-m$ the **additive inverse** of m.

G4 *Associativity* For all $m, n, p \in \mathbb{Z}$,
$$m + (n + p) = (m + n) + p,$$
so $+$ is associative.

Hence $(\mathbb{Z}, +)$ satisfies the group axioms, and so forms a group.

Notice, in this example, that we did *not* use the notation m^{-1} for the inverse of m, which would have been confusing.

By contrast, the set $\mathbb{Z}$ does *not* form a group under the operation of multiplication $\times$. Actually, the axioms G1, G2 and G4 do hold, with 1 as identity, but G3 fails. For example, the integer 2 has no inverse in $\mathbb{Z}$ under multiplication, because the equation $2n = 1$ has no solution for n in $\mathbb{Z}$.

In order to obtain a group whose elements are numbers and whose operation is $\times$, we certainly need to remove the number 0 (which will never have an inverse when the operation is $\times$). We also need a set of numbers that is closed under reciprocation; that is, if x is in the set, then so is $1/x$. Here is one example of such a group.

Activity 2.3 A group under multiplication

Let $\mathbb{R}^*$ denote the set of non-zero real numbers. Show that $(\mathbb{R}^*, \times)$ is a group.

A solution is given on page 52.

The use of $*$ as a superscript to denote the removal of 0 from a set will occur again later in the section.

The fundamental properties of arithmetic lead to many sets of numbers forming groups under $+$ and $\times$. We now list some of the main ones.

integers	$\mathbb{Z}$	
rational numbers	$\mathbb{Q}$	Each is a group under $+$,
real numbers	$\mathbb{R}$	with identity 0.
complex numbers	$\mathbb{C}$	
non-zero rational numbers	$\mathbb{Q}^*$	
non-zero real numbers	$\mathbb{R}^*$	Each is a group under $\times$,
non-zero complex numbers	$\mathbb{C}^*$	with identity 1.

You may ask, at this point, what *use* it is to know that these sets form groups under the given operations. Certainly, if you only wish to do arithmetic, then the answer is 'not much', since the group axioms merely restate rules of arithmetic. But if you want to understand how arithmetic works, and to use this understanding to illuminate other mathematical structures, then the idea of a group forms a valuable unifying concept.

These groups of numbers differ from the symmetry group $S(\square)$ discussed earlier in two important respects. First, they each have infinitely many elements, whereas $S(\square)$ has just eight elements. A group G with only finitely many elements is called a **finite group**, or a group of **finite order**, and the number of elements in G is called the **order** of G, denoted by $|G|$. For example, $|S(\square)| = 8$ and $|S(\triangle)| = 6$. Otherwise, G is called an **infinite group**, or a group of **infinite order**. For example, $(\mathbb{Z}, +)$ is a group of infinite order.

The second difference is slightly less obvious. Each of the groups of numbers described above has the property that the *order* in which the elements (numbers) are combined does not matter, but this is not true for $S(\square)$. For example,

$$r_{\pi/2} \circ q_0 = q_{\pi/4} \quad \text{but} \quad q_0 \circ r_{\pi/2} = q_{3\pi/4}.$$

A group $(G, *)$ with the additional property that, for all $g, h \in G$,

$$g * h = h * g,$$

is called an **Abelian group**, or **commutative group**, after the Norwegian mathematician Niels Henrik Abel (1802–1829). For example, $(\mathbb{Z}, +)$ is Abelian, but $(S(\square), \circ)$ is non-Abelian.

The examples given so far might suggest that the ideas of 'infinite' and 'Abelian' groups are directly related, but this is not the case. For example, the symmetry group $(S(\bigcirc), \circ)$ of a disc with centre the origin is of infinite order (it includes all rotations $r_\theta, 0 \le \theta < 2\pi$, and all reflections $q_\phi, 0 \le \phi < \pi$), but is non-Abelian. On the other hand, the finite set $\{1, -1\}$ forms a group under the operation $\times$, and this group is Abelian.

2.3 More groups

So far the only groups you have met are the symmetry groups of plane sets, and various groups of numbers under the operations $+$ and $\times$.

In Chapter D2, we studied the addition and multiplication tables for $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. There we saw that the addition tables for $\mathbb{Z}_n$ had the 'constant diagonal' pattern illustrated in Table 1.2. No general pattern was observed in the multiplication tables for $\mathbb{Z}_n$. However, we did find that if n is a *prime number*, then each non-zero row of the multiplication table for $\mathbb{Z}_n$ includes all the elements of $\mathbb{Z}_n$. These properties are illustrated for $n = 5$ below.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Before discussing whether $\mathbb{Z}_5$ is a group under $+_5$, or under $\times_5$, we make some general remarks about checking the group axioms. If a finite set G with associated operation $*$ is given, and we wish to check whether $(G, *)$ is a group, then a number of the axioms can be checked by compiling the table of elements of the form $g * h$, where $g, h \in G$. We continue to call such a table a Cayley table of G, and emphasise that the elements of G may be listed in any order, but that the order must be the *same* on both borders of the table. Also, it is convenient to place the identity element first. when this is known.

In terms of a Cayley table for G, the axioms G1, G2, G3 can be interpreted in the following more informal ways.

Closure (Axiom G1)

> Only elements of G appear in the body of the table.

Identity (Axiom G2)

> There is an element of G, called the identity, whose corresponding row and column repeat the borders of the table exactly.

Inverses (Axiom G3)

> The identity appears in each row of the table, and in each column, and these appearances are symmetric about the main diagonal.

To justify this third statement, recall that axiom G3 states that, for each element g in G, we can find g^{-1} such that

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

Hence e must appear at the intersection of row g and column g^{-1}, and also at the intersection of row g^{-1} and column g. Since the elements of G are taken in the same order on both borders, the elements $g \circ g^{-1}$ and $g^{-1} \circ g$ appear in the table in symmetric positions about the main diagonal (see Figure 2.2), leading to the rephrasing of axiom G3 given above.

Figure 2.2

Unfortunately, axiom G4 is tedious to check from a Cayley table. However, in appropriate cases, we can deduce that G4 holds using one of the following facts:

(a) addition and multiplication of numbers are both associative;

(b) the operations $+_n$ and $\times_n$ are both associative on $\mathbb{Z}_n$;

(c) composition of functions is associative;

(d) addition and multiplication of matrices are both associative.

There is no pattern to look for which gives associativity.

Property (b) was checked in Chapter D2, Subsection 3.1.

Notice, however, that the Cayley table of a finite group G *can* be used to check whether G is Abelian; this corresponds to the *whole* table being symmetric about the main diagonal.

Activity 2.4   Checking that a group is Abelian

Check that $(\{1, -1\}, \times)$ forms an Abelian group. (First, form a Cayley table for $(\{1, -1\}, \times)$.)

A solution is given on page 53.

Now look back at the addition table for $\mathbb{Z}_5$. Certainly, all the elements appearing in the table are in $\mathbb{Z}_5$, and 0 acts as identity and appears symmetrically in each row and column, so axioms G1, G2 and G3 hold. Also, axiom G4 holds in $\mathbb{Z}_5$ with the operation $+_5$, and so $(\mathbb{Z}_5, +_5)$ is indeed a group. Similarly, $(\mathbb{Z}_n, +_n)$ is a group for $n \geq 2$.

On the other hand, the multiplication table for $\mathbb{Z}_5$ indicates that $\mathbb{Z}_5$ is not a group under $\times_5$. Although G1 holds, G2 holds with $e = 1$ and G4 holds, the axiom G3 fails because 0 has no inverse. However, there seems to be a good chance that the smaller set $\{1, 2, 3, 4\}$ will form a group under $\times_5$. Its Cayley table is as follows.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Certainly all the elements appearing in the table are in the set $\{1, 2, 3, 4\}$. The element 1 acts as identity and appears symmetrically in each row and column, so G1, G2 and G3 hold. Also G4 holds, since $\times_5$ is associative on $\mathbb{Z}_5$ and so on $\{1, 2, 3, 4\}$. Thus this set is indeed a group under $\times_5$.

Generalising, we define $\mathbb{Z}_n^*$ to be the set $\mathbb{Z}_n$ with 0 removed:

$$\mathbb{Z}_n^* = \{1, 2, \ldots, n - 1\}.$$

For example, $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ and $\mathbb{Z}_2^* = \{1\}$.

It is tempting to think that $\mathbb{Z}_n^*$ will always be a group under the operation $\times_n$ but the Cayley table of $\mathbb{Z}_6^*$ indicates a new difficulty; the number 0 appears in the table, so G1 fails.

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

In fact, the number 0 appears in row a whenever a is not coprime with n. The only way to avoid having rows of this type is to insist that n is prime (as $n = 5$ is). This ensures that 1 appears in each row, and in each column. Therefore we deduce part (b) of the following theorem.

Theorem 2.3   Groups under modular arithmetic

(a) For $n \geq 2$, $\mathbb{Z}_n$ is an Abelian group under $+_n$.

(b) For each prime number p, $\mathbb{Z}_p^*$ is an Abelian group under $\times_p$.

These groups are Abelian because the operations $+$ and $\times$ are commutative, from which it follows that, for all a, b in $\mathbb{Z}_n$,

$$a +_n b = b +_n a \quad \text{and} \quad a \times_n b = b \times_n a.$$

As well as these, there are many other groups under modular addition or modular multiplication, some rather unexpected.

Activity 2.5   Other groups under modular arithmetic

Which of the following are groups?

(a) $\{1, 3, 5, 7\}$ under $\times_8$

(b) $\{2, 4, 6, 8\}$ under $+_{10}$

(c) $\{2, 4, 6, 8\}$ under $\times_{10}$

(In each case, compile a Cayley table, and use it to check axioms G1–G3. Note that in order to conclude that a given set and operation do *not* form a group, you only need to find one axiom that fails.)

Solutions are given on page 53.

We hope that Activity 2.5(c) will have convinced you that appearances can be deceptive where groups are concerned!

We end this subsection by briefly discussing groups whose elements are matrices. As you saw in Block B, matrices can be combined using the operations of matrix addition and multiplication, illustrated below using 2×2 matrices:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix},$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

The matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

act as identities for matrix addition and multiplication, respectively. The additive inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by

$$-\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

and, provided that $ad - bc \neq 0$, its multiplicative inverse is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Finally, both matrix addition and matrix multiplication are associative. It follows that many groups of matrices exist. For example, the set of all 2×2 matrices forms a group under addition, with identity $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, and the set of invertible matrices forms a group under multiplication, with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. These groups are infinite, but there are also many finite

See MST121 Chapter B2, Section 2.

groups of matrices. Consider, for example, the set whose elements are the four matrices

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Under matrix multiplication, the Cayley table for this set can be found by doing calculations such as

$$\mathbf{AB} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{C},$$

to obtain the following table.

$\times$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{I}$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{A}$	$\mathbf{A}$	$\mathbf{I}$	$\mathbf{C}$	$\mathbf{B}$
$\mathbf{B}$	$\mathbf{B}$	$\mathbf{C}$	$\mathbf{I}$	$\mathbf{A}$
$\mathbf{C}$	$\mathbf{C}$	$\mathbf{B}$	$\mathbf{A}$	$\mathbf{I}$

All the entries in the table do lie in the set $\{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$. The matrix $\mathbf{I}$ acts as an identity, and it appears symmetrically in each row and column. So axioms G1, G2 and G3 hold. Finally, matrix multiplication is known to be associative, so G4 also holds. Hence $\{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ is a group under matrix multiplication.

Actually, this group $\{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ is not as new as it may seem. Each of these matrices represents a plane isometry:

> $\mathbf{I}$ represents e, the identity;
> $\mathbf{A}$ represents q_0, reflection in the x-axis;
> $\mathbf{B}$ represents r_π, rotation by π about the origin;
> $\mathbf{C}$ represents $q_{\pi/2}$, reflection in the y-axis.

We already know that $\{e, q_0, r_\pi, q_{\pi/2}\}$ forms a group under the operation of composition because $\{e, q_0, r_\pi, q_{\pi/2}\} = S(\square)$. Since multiplication of matrices is equivalent to composition of the corresponding isometries, it was to be expected that $\{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ forms a group under matrix multiplication, corresponding to $(S(\square), \circ)$.

Here is a similar example for you to try.

Activity 2.6   A matrix group

Let

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{C} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(a) Show that $M = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ forms a group under matrix multiplication.

(b) Find a symmetry group corresponding to $(M, \times)$.

Solutions are given on page 53.

The Cayley table found in Activity 2.6 has a pattern which might be familiar to you from elsewhere. In Section 3 we take up the question of when two groups are 'different yet the same'.

If we need to check whether an infinite set forms a group, we do not have the option of examining a Cayley table. Often, though, we are dealing with an operation that we already know to be associative. In that case, we only need to check the other three group axioms.

Activity 2.7   Checking for infinite groups

(a) Show that the set H, consisting of 2×2 matrices of the form

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix},$$

where $a \in \mathbb{R}$, forms a group under matrix addition.

(b) Show that the set

$$B = \mathbb{Z} \cup \{1/m : m \in \mathbb{Z}, m \neq 0\},$$

consisting of integers together with reciprocals of non-zero integers, does *not* form a group under addition.

For two sets A and B, the set $A \cup B$ is the **union** of A and B; it consists of all the elements of both A and B.

Comment

(a) Addition of matrices is associative, so axiom G4 holds. To check that the set is closed under matrix addition, consider the sum of two matrices of the given form. We have

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a+b \\ 0 & 0 \end{pmatrix},$$

which again is in H. So the set H is closed under addition, confirming axiom G1. The identity for matrix addition is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, and this is of the given form (with $a = 0$), and so is in H, confirming axiom G2. The additive inverse of the matrix $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$ is $\begin{pmatrix} 0 & -a \\ 0 & 0 \end{pmatrix}$, and this inverse also lies in H, confirming axiom G3.

Hence the set H does form a group under matrix addition.

(b) The set B is not closed under addition (although the other axioms do hold). For example, both 2 and $\frac{1}{3}$ are in the set B, but

$$2 + \tfrac{1}{3} = \tfrac{7}{3}$$

is not in B. Since axiom G1 does not hold, B does not form a group under addition.

In Activity 2.7(a), the set H is a subset of the set of all 2×2 matrices, which we already know to form a group under addition. In general, suppose that $(G, *)$ is a group, and H is a subset of G satisfying the following three conditions.

◇   The operation $*$ is closed on H.

◇   The identity element of G is in H.

◇ H is closed under inverses; that is, if a is in H, then its inverse in G, a^{-1}, is also in H.

Then we can deduce that H must also be a group under $*$. (Associativity of $*$ on H follows from associativity of $*$ on G.) In this case, we say that $(H, *)$ forms a **subgroup** of $(G, *)$.

2.4 Some properties of all groups

Axiom G2 for a group $(G, *)$ asserts that there must be an identity element, e, in the group. The axiom does *not* state that this identity must be unique. Could a group have two different identity elements? If so, then each would have the property that, for all g in G,

$$g * identity = g = identity * g.$$

This cannot happen, as we now show.

Suppose that e and e' are both identities of G. Then

$$e * e' = e' \text{ (since } e \text{ is an identity), and } e * e' = e \text{ (since } e' \text{ is an identity).}$$

Thus $e' = e$, and so G has just one identity.

Axiom G3 guarantees that each group element has an inverse, but does not state that this inverse must be unique. However, a similar argument shows that uniqueness of inverses does hold in a general group.

Activity 2.8   Uniqueness of inverses

Prove that each element g of a group $(G, *)$ has a unique inverse element; that is, show that there cannot be two different group elements h and h' for which $h * g = e = g * h$ and $h' * g = e = g * h'$. To do this, suppose that h and h' are both inverses of g and consider the equation $(h * g) * h' = h * (g * h')$.

A solution is given on page 53.

The uniqueness of the identity, and of inverses, are convenient properties of a group. It might seem more sensible to specify this uniqueness when stating the group axioms. But if we had done that, then more work would be required every time we want to show that a particular set and operation form a group. It is preferable to assume as little as possible in the basic group axioms, and to deduce other results such as these as theorems.

The Cayley tables of the groups you have met in this section suggest another property of all groups. You may well have noticed that, in each table, every element of the group appears exactly once in each row and column of the body of the table. We now indicate how to deduce this property from the group axioms.

Suppose that $(G, *)$ is a finite group and we wish to show that row g, say, includes an element, h say, from G. As indicated in Figure 2.3, we need to find an element x of G such that

$$g * x = h.$$

In essence, this is an equation for an unknown element x, which we have to solve to find x in terms of the known elements g and h. Since G is a group, g has an inverse g^{-1}. If we apply g^{-1} to the left of both sides of $g * x = h$, then we obtain

$$g^{-1} * (g * x) = g^{-1} * h.$$

By axiom G4, the left-hand side is $(g^{-1} * g) * x = e * x = x$, so

$$x = g^{-1} * h.$$
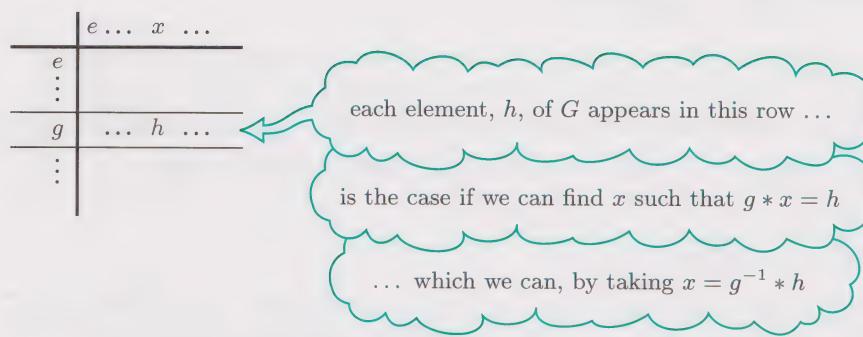
Figure 2.3 Every element of a finite group appears in each row of its Cayley table

This manipulation shows that the only possible solution of the equation $g * x = h$ is $x = g^{-1} * h$, and this value of x is indeed a solution because

$$g * x = g * (g^{-1} * h) = (g * g^{-1}) * h = e * h = h.$$

The above reasoning shows that the element h appears in row g of the Cayley table for G, and does so in precisely one position, namely in column $g^{-1} * h$. Since g and h were any elements of G, we deduce that each element of G appears exactly once in each row of the body of the Cayley table. A similar reasoning, with the equation $x * g = h$, leads to the corresponding result for columns.

This 'once in each row and column' property severely restricts the way in which a Cayley table for a finite group can be completed. For example, if $G = \{e, a\}$ is a group under the operation $*$, with identity e, then its Cayley table must take the form shown in the margin.

$*$	e	a
e	e	a
a	a	?

The 'once in each row and column' property then implies that the missing element in the bottom right corner must be e.

Activity 2.9 Completing a Cayley table

Complete the following Cayley table in the only way possible if $(\{e, a, b, c\}, *)$ is a group.

$*$	e	a	b	c
e	e	a	b	?
a	a	?	?	b
b	?	c	?	?
c	c	?	?	a

In Section 3, you will see that $(\{e, a, b, c\}, *)$ is indeed a group.

A solution is given on page 54.

Earlier in this subsection you saw that the axioms for a group allow us to solve simple equations of the form $g * x = h$ (or indeed $x * g = h$). Very similar reasoning shows that every group $(G, *)$ has what is known as the *cancellation property*; namely, for g, h and k in G:

The cancellation property will be useful in Section 3.

if $k * g = k * h$, then $g = h$;

if $g * k = h * k$, then $g = h$.

To prove these, you need only apply the inverse k^{-1} to the equations, on the left or the right as appropriate.

Summary of Section 2

A set together with a binary operation forms a group if four axioms are satisfied: closure; the existence of an identity; the existence of inverses; and associativity. You met a number of examples of groups, in particular:

◇   symmetries of a plane set, with composition of functions;

◇ $(\mathbb{Z}_n, +_n)$;

◇ $(\mathbb{Z}_p^*, \times_p)$, where p is prime;

as well as some infinite groups such as $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \times)$. If the group operation is commutative, then we say that the group is Abelian.

For a small finite set, a Cayley table can provide a convenient way of checking three of the group axioms (but not associativity). We know from previous work that a number of operations *are* associative, including composition of functions, modular addition and multiplication, and addition and multiplication of real and complex numbers, and of matrices.

Exercises for Section 2

Exercise 2.1

Show that each of the following sets forms a group under the given operation.

(a) The set of even integers $\{2n : n \in \mathbb{Z}\}$ under $+$.

(b) The set $\{1, 5, 7, 11\}$ under $\times_{12}$.

(c) The set of complex numbers $\{1, -1, i, -i\}$ under $\times$.

(d) The set of matrices $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R} \right\}$ under $\times$.

(e) The set $\{1, 2, 4, 5, 7, 8\}$ under $\times_9$.

(f) The set $\{3, 6, 9, 12\}$ under $\times_{15}$.

Exercise 2.2

Let $(G, *)$ be a group, with g and h elements of G.

(a) Show that the inverse of g^{-1} is g.

(b) Show that the inverse of $g * h$ is $h^{-1} * g^{-1}$.

(c) Show that if g, h and $g * h$ are all self-inverse, then $g * h = h * g$.

3 Isomorphic groups

3.1 Matching Cayley tables

In this section, we examine the idea of two groups being 'essentially the same'. We shall confine our attention to groups of finite order. Compare, for example, the Cayley tables given in Tables 3.1 and 3.2, for $(\mathbb{Z}_4, +_4)$ and $(M, \times)$, where $M = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ is the group of matrices considered in Activity 2.6.

Table 3.1 Cayley table for $(\mathbb{Z}_4, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 3.2 Cayley table for $(M, \times)$

$\times$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{I}$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{A}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$	$\mathbf{I}$
$\mathbf{B}$	$\mathbf{B}$	$\mathbf{C}$	$\mathbf{I}$	$\mathbf{A}$
$\mathbf{C}$	$\mathbf{C}$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$

These tables both show the pattern of 'constant diagonals' (as in Table 1.2). What is more, we can match them in a detailed way. To match the borders of Table 3.1 with those of Table 3.2, we need only to replace

0 by $\mathbf{I}$,   1 by $\mathbf{A}$,   2 by $\mathbf{B}$,   3 by $\mathbf{C}$,

and the operation $+_4$ by matrix multiplication. If we make these replacements in the body of Table 3.1, then the results match *every* entry in Table 3.2. (Look, for example, at the entries in the tinted boxes in the two tables.)

This process of matching can be formalised by introducing a function ϕ between $\mathbb{Z}_4$ and M, defined as follows:

$$\phi(0) = \mathbf{I}, \quad \phi(1) = \mathbf{A}, \quad \phi(2) = \mathbf{B}, \quad \phi(3) = \mathbf{C}.$$

This function converts every entry in Table 3.1 to the entry in the corresponding position in Table 3.2.

In general, whenever $(G, *)$ and $(H, \diamond)$ are finite groups, and $\phi : G \to H$ is a one-one function from G onto H that converts a Cayley table of $(G, *)$ to a Cayley table of $(H, \diamond)$, then ϕ is called an **isomorphism** and the two groups are said to be **isomorphic** to each other. For example, the groups $(\mathbb{Z}_4, +_4)$ and $(M, \times)$ are isomorphic to each other.

Here, $\diamond$ represents another binary operation.

From the Greek: isos meaning equal, and morpho meaning form.

Activity 3.1   Matching Cayley tables

(a) Compare the Cayley tables for $(\mathbb{Z}_4, +_4)$ and for the set of symmetries of the wheel trim $S(\text{TRIM}) = \{e, r_{\pi/2}, r_\pi, r_{3\pi/2}\}$ under composition. Give an isomorphism between the groups $(\mathbb{Z}_4, +_4)$ and $(S(\text{TRIM}), \circ)$.

See Table 3.1 and the solution to Activity 1.8.

(b) Look at the Cayley table for $(S(\triangle), \circ)$, given in the Comment on Activity 1.7(c). Part of that table has the same pattern as the Cayley table of $(\mathbb{Z}_3, +_3)$. Identify a subgroup of $(S(\triangle), \circ)$ that is isomorphic to $(\mathbb{Z}_3, +_3)$, and give an isomorphism from $\mathbb{Z}_3$ to that subgroup.

Solutions are given on page 54.

Activity 3.2   Symmetry groups isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$

Find plane sets, whose only symmetries are rotations, and which have symmetry groups that are isomorphic to each of:

(a) $(\mathbb{Z}_2, +_2)$,   (b) $(\mathbb{Z}_3, +_3)$.

(*Hint:* In part (a) you need to choose a set with just one symmetry apart from the identity.)

Solutions are given on page 54.

Sometimes, an isomorphism between two groups exists, but is not immediately obvious. Consider, for example, the following Cayley tables of the groups $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

As written above, the Cayley tables do not show the same pattern. For example, the one on the left has the 'constant diagonal' property, but the one on the right does not. However, if we rearrange the table for $\mathbb{Z}_5^*$, by exchanging the positions of 3 and 4 on both borders, then an isomorphism becomes apparent.

$\times_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Now the table for $\mathbb{Z}_5^*$ does have 'constant diagonals', and an isomorphism ϕ from $(\mathbb{Z}_4, +_4)$ to $(\mathbb{Z}_5^*, \times_5)$ can be defined by:

$$\phi(0) = 1, \quad \phi(1) = 2, \quad \phi(2) = 4, \quad \phi(3) = 3.$$

In looking for an isomorphism between $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_5^*, \times)$, how might one see that it is appropriate to exchange 3 and 4 in $\mathbb{Z}_5^*$ in this way? A clue can be found by looking at the main diagonals in the two Cayley tables. That for $\mathbb{Z}_4$ has an alternating pattern: $0, 2, 0, 2$. Originally, the main diagonal for $\mathbb{Z}_5^*$ showed a different pattern: $1, 4, 4, 1$. If we reorder the elements of $\mathbb{Z}_5^*$, the same four elements will appear on the main diagonal of the Cayley table, but in a different order. In seeking to order the elements of $\mathbb{Z}_5^*$ so as to match the Cayley tables, we *must* start with the identity element, 1, so that the first row and first column will repeat the borders, as in the Cayley table for $\mathbb{Z}_4$. So the only orders for $\mathbb{Z}_5^*$ which would lead to matching main diagonals and thus might lead to an isomorphism are:

$$1, 2, 4, 3 \quad \text{and} \quad 1, 3, 4, 2.$$

We saw above that the order $1, 2, 4, 3$ leads to an isomorphism. It turns out that $1, 3, 4, 2$ does also, the isomorphism being given by the function $\psi(0) = 1, \psi(1) = 3, \psi(2) = 4, \psi(3) = 2$. Notice that it is possible to have more than one isomorphism between the same two groups. (We shall often find that where there is one isomorphism, then there are others, as well.)

The next activity invites you to find such a rearrangement.

Activity 3.3   Rearranging Cayley tables

In Activity 2.5(c), a Cayley table of the group $(\{2, 4, 6, 8\}, \times_{10})$ was found, as below.

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

Show that this Cayley table can be rearranged so that its pattern is the same as that of the Cayley table of $(\mathbb{Z}_4, +_4)$. Write down the corresponding isomorphism. (Remember that the identity of this group is 6.)

A solution is given on page 55.

3.2   Properties of isomorphic groups

Isomorphism makes formal the idea of two groups being 'essentially the same'. If groups G and H can be matched up, element by element, so that their Cayley tables are the same, then *as groups* G and H are identical; that is, G and H will have exactly the same group properties. Anything that we might observe about the structure of G will be reflected in the structure of H (and vice versa). For example, isomorphic groups must have the same number of members, and if one group is Abelian then the other must also be Abelian. The following result summarises some of the basic properties shared by isomorphic groups.

Theorem 3.1   Properties preserved by isomorphism

Let $(G, *)$ and $(H, \diamond)$ be finite groups which are isomorphic to each other. Then:

(a) $|G| = |H|$;

(b) G and H have the same number of self-inverse elements;

(c) G is Abelian if and only if H is Abelian.

Recall that $|G|$ denotes the order of G, that is, the number of elements in G.

Property (a) holds because an isomorphism from G to H is a function which is one-one and onto, so G and H must have the same number of elements.

To see why property (b) holds, note that an element g of a group is self-inverse if and only if the identity e appears at the intersection of row g and column g on the main diagonal of the Cayley table of G. Thus the number of self-inverse elements is the same as the number of occurrences of e on the main diagonal of the Cayley table, and this must be the same for both G and H.

Finally, property (c) holds because a finite group is Abelian if and only if its Cayley table is symmetric about the main diagonal, and one Cayley table has this property if and only if the other does.

Theorem 3.1 is particularly useful when we want to show that two groups G and H are *not* isomorphic. For example, property (a) shows that if G and H have a different number of elements, then they are not isomorphic to each other. We now show how property (b) can be used in a similar way.

You have now seen several groups of order 4 which are isomorphic to each other, and you may have begun to suspect that all groups of order 4 are isomorphic to $(\mathbb{Z}_4, +_4)$. However, consider the Cayley table of the symmetry group $(S(\square), \circ)$.

$\circ$	e	r_π	q_0	$q_{\pi/2}$
e	e	r_π	q_0	$q_{\pi/2}$
r_π	r_π	e	$q_{\pi/2}$	q_0
q_0	q_0	$q_{\pi/2}$	e	r_π
$q_{\pi/2}$	$q_{\pi/2}$	q_0	r_π	e

The presence of the identity e everywhere on the main diagonal indicates that all four elements of $S(\square)$ are self-inverse. Hence, by Theorem 3.1(b), $(S(\square), \circ)$ is not isomorphic to $(\mathbb{Z}_4, +_4)$, which has only two self-inverse elements (0 and 2). Other differences in the patterns can be found, but the number of self-inverse elements is an easy difference to notice and state.

Theorem 3.1 is less useful if we want to show that two groups *are* isomorphic, as in the next activity.

Activity 3.4   Finding isomorphic groups

Which of the two groups found in Activity 2.5 is isomorphic to $(S(\square), \circ)$?

(*Hint:* You need to study the Cayley tables of the two groups, to see which one matches the Cayley table of $S(\square)$.)

A solution is given on page 55.

In the next activity, we ask you to consider isomorphisms between groups of order 6.

Activity 3.5   Groups of order 6

(a) Give one reason why the groups $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$ are not isomorphic to each other.

(b) Find a plane set whose symmetry group is isomorphic to $(\mathbb{Z}_6, +_6)$.

(*Hint:* In part (a), try using Theorem 3.1, and in part (b) consider the approach in the solution to Activity 3.2(b).)

Solutions are given on page 55.

3.3 Groups of small order

So far we have met two different types of group of order 4, those isomorphic to $(\mathbb{Z}_4, +_4)$ and those isomorphic to $(S(\square), \circ)$. It is natural to ask whether there is yet another type of group of order 4, isomorphic to neither of these. We now show that there is not.

Theorem 3.2   Groups of order 4

Any group of order 4 is isomorphic either to $(\mathbb{Z}_4, +_4)$ or to $(S(\square), \circ)$.

In the proof we assume that $(G, *)$ is a group of order 4, with elements named e (the identity), a, b and c. We want to show that the Cayley table of $(G, *)$ can be arranged to match either that of $(\mathbb{Z}_4, +_4)$ or that of $(S(\square), \circ)$.

We use a simple but very useful fact about self-inverse elements.

Lemma 3.1   Self-inverse elements

If $(G, *)$ is a finite group, then the number of elements of $(G, *)$ which are not self-inverse is even.

It is conventional to regard 0 as an even number.

This result holds because an element g which is not self-inverse has a unique inverse g^{-1}, with $g^{-1} \neq g$. Also, the inverse of g^{-1} is g. Thus the elements which are not self-inverse form pairs, so there must be an even number of them.

In our group G of order 4, the number of self-inverse elements must also be even by Lemma 3.1, and so it is equal to 2 or 4 (because e itself is self-inverse). Thus either exactly one of a, b, c is self-inverse, say a, or they are all self-inverse, and so there are two cases to consider:

If n is even, then $4 - n$ is also even.

    Case 1: $a * a = e$ and $b * c = e = c * b$,

    Case 2: $a * a = e$, $b * b = e$ and $c * c = e$.

In Case 1, $b^{-1} \neq b$, while $a^{-1} = a$ and $e^{-1} = e$. Hence b^{-1} must be c.

The corresponding Cayley tables must then have the following entries.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	?	e
c	c	?	e	?

Case 1

$*$	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	e	?
c	c	?	?	e

Case 2

We can complete these tables using the 'once in each row and column' property. In both cases, the entry in row a, column b is none of a, e or b, so it must be c. Using the same property, the remaining entries in the two cases then follow.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Case 1

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Case 2

$*$	e	b	a	c
e	e	b	a	c
b	b	a	c	e
a	a	c	e	b
c	c	e	b	a

Case 1

The Cayley table in Case 2 has the same pattern as the Cayley table of $(S(\square), \circ)$. An isomorphism is provided in this case by: $\phi(e) = e$, $\phi(a) = r_\pi$, $\phi(b) = q_0$, $\phi(c) = q_{\pi/2}$. In Case 1, if the elements are arranged in the order: e, b, a, c, then the Cayley table shows the constant diagonal pattern. So $\psi(e) = 0$, $\psi(b) = 1$, $\psi(a) = 2$, $\psi(c) = 3$ provides an isomorphism with $(\mathbb{Z}_4, +_4)$.

Hence any group G of order 4 is isomorphic either to $(\mathbb{Z}_4, +_4)$ or to $(S(\square), \circ)$, and the proof is complete.

Incidentally, their Cayley tables show that both the groups $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$ are Abelian. Thus, by Theorems 3.1(c) and 3.2, *all* groups of order 4 are Abelian.

Having seen that there are only two types of groups of order 4, we may ask how many types of groups there are of any given order n. Such information is useful when a finite group arises in a new context, and much work has been done to answer the question. The table below gives the number of different types of group of orders up to 15, and even this short table shows that there is unlikely to be a simple formula for the number of different types of group of order n.

Order n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Group types	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

$*$	e
e	e

The entry in the first column of this table is clear. Any group with exactly one element must consist of an identity e with the Cayley table shown in the margin. All such groups are evidently isomorphic to each other.

Activity 3.6   Groups of orders 2 and 3

Show that:

(a) all groups of order 2 are isomorphic to $(\mathbb{Z}_2, +_2)$;

(b) all groups of order 3 are isomorphic to $(\mathbb{Z}_3, +_3)$.

Solutions are given on page 56.

The table above indicates that there is only one type of group of order 5. Since $(\mathbb{Z}_5, +_5)$ has order 5, this means that *all* groups of order 5 must be isomorphic to $(\mathbb{Z}_5, +_5)$. Similarly, all groups of order 7 must be isomorphic to $(\mathbb{Z}_7, +_7)$. These are both special cases of a general result which states that if p is a prime number, then all groups of order p are isomorphic to $(\mathbb{Z}_p, +_p)$; proving this result is not especially difficult, but we do not have the space for it here.

See Activity 3.5(a).

The table also shows that there are two essentially different groups of order 6. Since $(\mathbb{Z}_6, +_6)$ and $(S(\triangle), \circ)$ both have order 6 and are not isomorphic to each other, it follows that all groups of order 6 must be isomorphic either to $(\mathbb{Z}_6, +_6)$ or to $(S(\triangle), \circ)$. This can be proved by reasoning which is similar to, but more complicated than, that used to prove Theorem 3.2.

The situation for groups of order 8 is rather more complicated, as there are five different types of groups of this order. So far you have met two groups of order 8 which are not isomorphic to each other. One is $(\mathbb{Z}_8, +_8)$ and the other is $(S(\square), \circ)$, whose Cayley table is given in Table 1.1. There are

three other types of group of order 8, but you have met none of these so far in this chapter. Two of these arise as the symmetry groups of the *three-dimensional* objects shown in Figure 3.1. The third has the Cayley table given below. The label × used for the operation, and the members of this group, $QUAT = \{1, -1, i, -i, j, -j, k, -k\}$, are no accident, but we shall not discuss that here.

×	1	−1	i	$-i$	j	$-j$	k	$-k$
1	1	−1	i	$-i$	j	$-j$	k	$-k$
−1	−1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	−1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	−1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	−1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	−1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	−1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	−1

The name *QUAT* refers to the *quaternions*, a generalisation of the complex numbers invented by W. R. Hamilton (1805–1865).

The group axioms G1, G2, G3 can be checked from this table. The axiom G4 needs to be checked case by case. For example,

$$i(jk) = i^2 = -1$$
$$(ij)k = k^2 = -1.$$

(a)   (b)

The symmetries of these sets are isometries of three dimensional space which map each set onto itself.
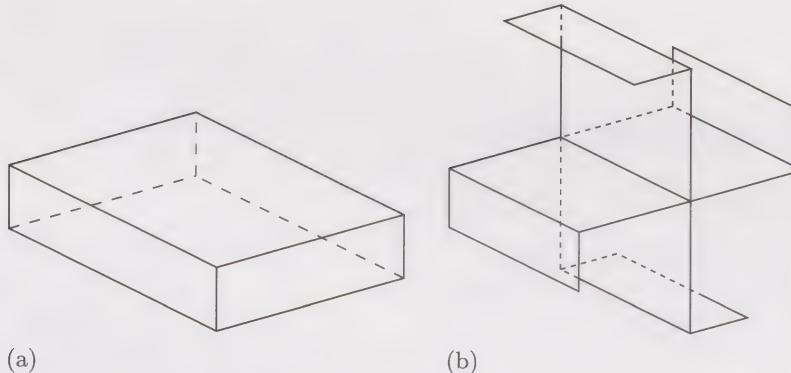
Figure 3.1   Two three-dimensional sets with groups of symmetries of order 8: (a) a box, (b) a rotor

We can tell that these groups of order 8 are not isomorphic to each other by counting the self-inverse elements in each, and by determining whether they are Abelian. This can be done by examining their Cayley tables, but we shall not do that here. However, for reference, this information is given in a table in the section summary.

Summary of Section 3

An isomorphism between finite groups $(G, *)$ and $(H, \diamond)$ is a function $f : G \longrightarrow H$ that is one-one and onto, and converts a Cayley table of $(G, *)$ to a Cayley table of $(H, \diamond)$. Isomorphic groups can be recognised by matching their Cayley tables, but it may be necessary to rearrange the order of the elements before a match can be seen.

If two groups are isomorphic to each other, then they share properties such as their order, the number of self-inverse elements each has, and whether they are Abelian. So if two groups differ in any of these features, then they are not isomorphic to each other.

We classified all groups of orders 1, 2, 3 and 4, and went on to assert that all groups of orders up to 8 are isomorphic to one of the groups given in the table below. If you encounter a group of order up to 8, then the properties shown in the table will help you recognise to which of these groups your group is isomorphic.

Group	Order	Self-inverses	Abelian
$(\{e\}, *)$	1	1	✓
$(\mathbb{Z}_2, +_2)$	2	2	✓
$(\mathbb{Z}_3, +_3)$	3	1	✓
$(\mathbb{Z}_4, +_4)$	4	2	✓
$(S(\square), \circ)$	4	4	✓
$(\mathbb{Z}_5, +_5)$	5	1	✓
$(\mathbb{Z}_6, +_6)$	6	2	✓
$(S(\triangle), \circ)$	6	4	×
$(\mathbb{Z}_7, +_7)$	7	1	✓
$(\mathbb{Z}_8, +_8)$	8	2	✓
$(S(\square), \circ)$	8	6	×
$(S(\text{BOX}), \circ)$	8	8	✓
$(S(\text{ROTOR}), \circ)$	8	4	✓
$(QUAT, \times)$	8	2	×

These entries refer to the box and rotor shown in Figure 3.1. The Cayley table for $QUAT$ is given on page 39.

Exercises for Section 3

Exercise 3.1

(a) A Cayley table for a group $G = \{a, b, c, d, e, f, g, h\}$ of order 8 is given here. What is the identity element of this group? To which of the groups tabulated in the summary of Section 3 is this group isomorphic?

*	a	b	c	d	e	f	g	h
a	e	c	b	h	a	g	f	d
b	c	e	a	f	b	d	h	g
c	b	a	e	g	c	h	d	f
d	h	f	g	e	d	b	c	a
e	a	b	c	d	e	f	g	h
f	g	d	h	b	f	e	a	c
g	f	h	d	c	g	a	e	b
h	d	g	f	a	h	c	b	e

(b) Consider each of the groups in Exercise 2.1, and determine to which, if any, of the groups tabulated in the summary of Section 3 it is isomorphic. Where a group from Exercise 2.1 is isomorphic to one of those in the table, give a specific isomorphism.

Exercise 3.2

The symmetry group $(S(\text{PENT}), \circ)$ of the regular pentagon has 10 elements (see the Comment for Activity 1.5(a)). Show that $(S(\text{PENT}), \circ)$ is not isomorphic to $(\mathbb{Z}_{10}, +_{10})$.

4   Groups in action

In this final section, we aim to indicate the wide range of possible applications of groups.

This section will not be assessed. It is included for your interest only!

4.1   Wheel trims and wallpapers

Throughout history an enormous range of patterns have been created to decorate objects. One way to *classify* such patterns is to use their symmetry groups.

First we consider the patterns which have been used to decorate bounded sets, such as car wheel trims, drain covers and rose windows (Figure 4.1).
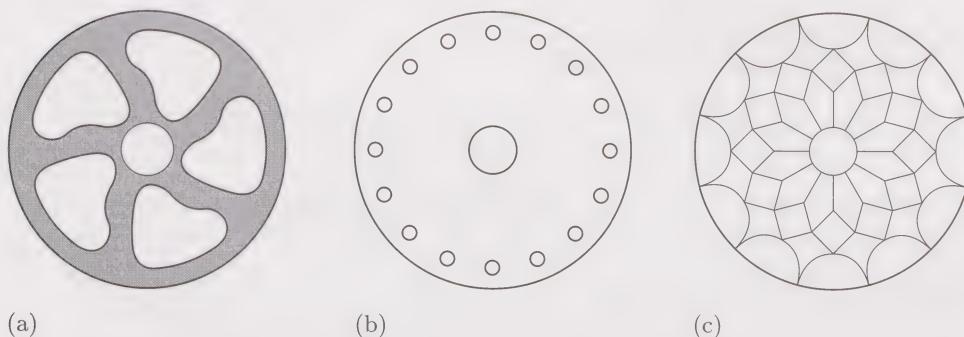
(a)   (b)   (c)

Figure 4.1   (a) A wheel trim   (b) A drain cover   (c) A rose window

Observation of such bounded sets indicates that their symmetry groups are always one of two types. The first type of symmetry group consists of a finite number, n say, of anticlockwise rotations through multiples of $2\pi/n$. This is the symmetry group of a regular polygon with n sides, which has been modified to retain the rotational symmetries but lose the reflectional ones. For $n = 6$, the set of symmetries is $\{e, r_{\pi/3}, r_{2\pi/3}, r_{\pi}, r_{4\pi/3}, r_{5\pi/3}\}$, shown in Figure 4.2(a).
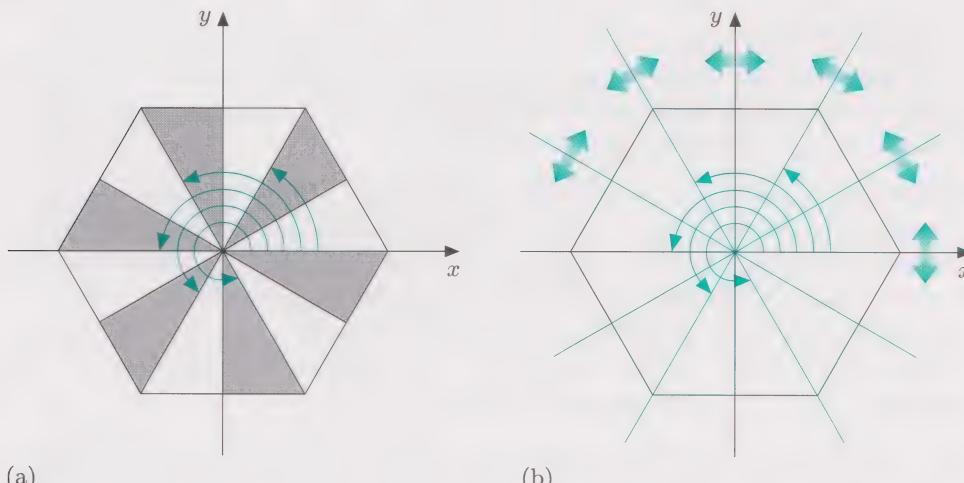
(a)   (b)

Figure 4.2   (a) Symmetries of a regular hexagon with shading to exclude reflectional symmetries   (b) All the symmetries of a regular hexagon

To help clarify the structure of this symmetry group, it is convenient to call the smallest non-trivial rotation $r = r_{2\pi/n}$ and introduce power notation for successive compositions:

$$r^2 = r \circ r, \quad r^3 = r \circ r \circ r, \ldots .$$

Then we must have $r^n = e$, and the symmetry group is of the form

$$\{e, r, r^2, \ldots, r^{n-1}\}. \tag{4.1}$$

A group of this type is called a **cyclic group of order n, generated by r**, because the successive powers of r cycle through all the elements of the group. Its Cayley table is of the form:

As a special case, a group $\{e\}$, consisting of just the identity, can be thought of as a **cyclic group of order** 1.

$\circ$	e	r	r^2	$\ldots$	r^{n-1}
e	e	r	r^2	$\ldots$	r^{n-1}
r	r	r^2	r^3	$\ldots$	e
r^2	r^2	r^3	r^4	$\ldots$	r
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
r^{n-1}	r^{n-1}	e	r	$\ldots$	r^{n-2}

Notice that this Cayley table has the constant diagonal pattern, which indicates that such a group is isomorphic to $(\mathbb{Z}_n, +_n)$.

The second type of symmetry group observed in bounded sets is the full symmetry group of a regular polygon with n sides. (The case $n = 6$ is illustrated in Figure 4.2(b).) This has $2n$ symmetries: the n rotations listed above and n reflections in axes through the centre of the set.

The structure of this group can also be clarified by writing $r = r_{2\pi/n}$, $q = q_{\pi/n}$, and using the power notation r^2, r^3, and so on. As above, $r^n = e$ and also $q^2 = e$, since q is a reflection. Using Table 1.3, it can be shown that the isometries

$$q, q \circ r, q \circ r^2, \ldots, q \circ r^{n-1}$$

are the n reflections of the regular polygon, and so this symmetry group can be written in the form

$$\{e, r, r^2, \ldots, r^{n-1}, q, q \circ r, q \circ r^2, \ldots, q \circ r^{n-1}\}. \tag{4.2}$$

The word dihedral means 'two-sided'.

A group with this structure is called a **dihedral group of order $2n$, generated by r and q**. Note that the group $S(\square) = \{e, r_\pi, q_0, q_{\pi/2}\}$ is not the symmetry group of a regular polygon (there is no regular polygon with two sides!), but it does have the structure in (4.2) with $n = 2$, and so is often called a **dihedral group of order** 4. Similarly $\{e, q_{\pi/2}\}$ may be thought of as a **dihedral group of order** 2.

Besides cyclic and dihedral groups, are there any other types of symmetry groups which can occur for bounded sets? Certainly the designers of wheel trims, drain covers and rose windows have not found any. In fact, it can be proved that if the symmetry group of a bounded plane set is *finite*, then that symmetry group is either a cyclic group of order n or a dihedral group of order $2n$, for some positive integer n. This demonstrates that the designers have not overlooked any patterns!

This result is typical of the way in which groups can be used to classify the possible structures, or patterns, in some family of objects. In this case of bounded sets, the possible symmetry groups are relatively easy to find, perhaps because we are so familiar with the objects in question. However, the following classification problems are more challenging.

In everyday language, a frieze is a decorative device consisting of a repeating pattern on a strip, such as that in Figure 1.1(e). Expressed mathematically, a **frieze** is a plane set whose symmetry group contains non-trivial translations in exactly one direction and which has a translation of shortest displacement. Thus both the sets in Figure 1.1(d) and (e) are friezes, in this mathematical sense. The symmetry group of a frieze is called a **frieze group**, and it must have infinitely many elements. For example, a typical symmetry of the ladder in Figure 1.1(d) is obtained by first performing one of the four symmetries of a single rectangle in the ladder and following this by one of the infinitely many possible translations. You have already seen that the symmetry groups of the two friezes in Figure 1.1(d) and (e) include different isometries, and it seems likely that a number of different types of frieze groups are possible.

In fact it can be shown that there are seven essentially different frieze groups, distinguished by the types of isometries which are present. The ladder (Figure 1.1(d)) has every type of symmetry possible in a frieze group. The other six types of frieze are illustrated in Figure 4.3. (We saw in Section 1 that the frieze in Figure 1.1(e) has two types of rotational symmetries but no reflectional symmetries, as does that in Figure 4.3(c).)

(a)   (b)   (c)

(d)   (e)   (f)
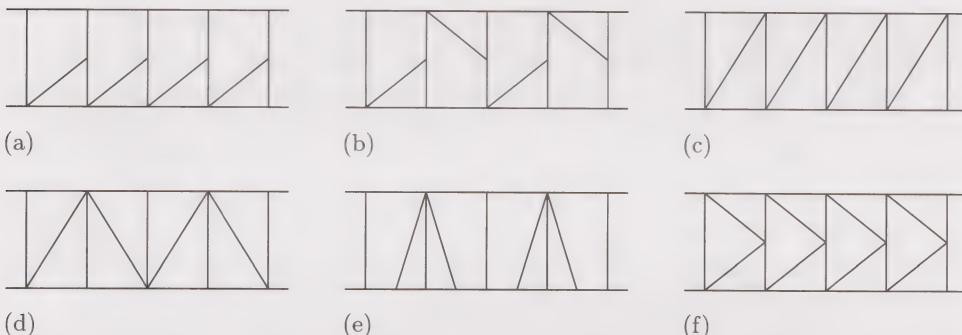
Figure 4.3   The six possible friezes, other than that in Figure 1.1(d)

A **wallpaper** is, in a mathematical sense, a plane set whose symmetry group contains non-trivial translations in at least *two* non-parallel directions and which has a translation of shortest displacement in each such direction. For example, a regular triangular grid or a square grid (see Figure 4.4) are both wallpapers.

(a)   (b)
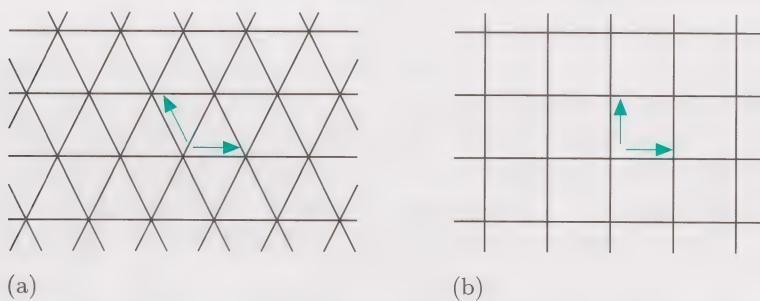
Figure 4.4   Two possible wallpapers: (a) a triangular grid,   (b) a square grid

The symmetry group of a wallpaper is called a **wallpaper group**, and it must have infinitely many elements. For example, a typical symmetry of the square grid is obtained by first performing one of the eight symmetries corresponding to a particular square of the grid and following this by one of the infinitely many possible translations. It seems likely that a large

number of different types of wallpaper group can occur and that their classification will be difficult.

The first complete classification of wallpaper groups was published by the Russian crystallographer E. S. Fedorov in 1891. Such groups arise naturally when studying the way in which repeating patterns occur within natural materials. Fedorov showed that every wallpaper group must be one of 17 essentially different types. Details from three possible wallpapers (other than those in Figure 4.4) are illustrated in Figure 4.5.

All of the 17 wallpaper groups can be found in decorations at the Alhambra, built in Spain by the Moors in the thirteenth century.


(a)   (b)   (c)
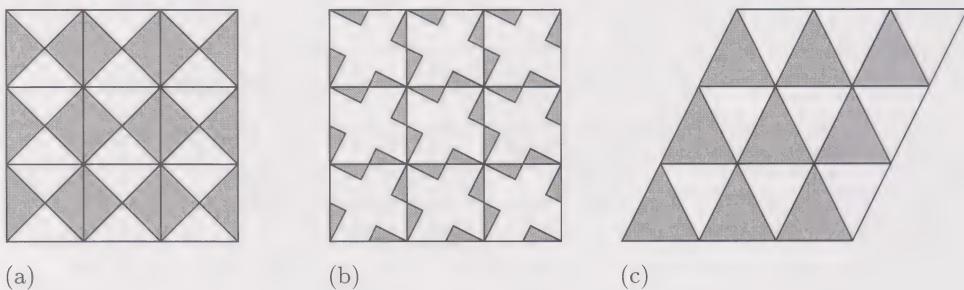
Figure 4.5   Three of the seventeen possible wallpapers

As you may imagine, proving that these 17 groups form a complete classification of the wallpaper groups is by no means easy. Imagine, then, how difficult is the corresponding problem for three-dimensional space, which is even more important to crystallographers. It turns out that there are exactly 230 **space groups**, as they are called. Their classification was carried out independently in the early 1890s by Fedorov in Russia, A. Schoenflies in Germany and W. Barlow in England. Earlier A. Bravais (1849) had shown that, if the only symmetries permitted are those that keep a particular point invariant, then there are 32 essentially different types of symmetry group, known as the **crystallographic groups**. These classifications are in regular use by crystallographers today.

4.2   Groups and physics

Physics aims to discover laws which model the behaviour of the physical world, from the universe to subatomic particles. Since many objects in the physical world display symmetry, and this usually has significance, it is not surprising that physicists have found groups useful.

That the language of groups is of value in classifying the structure of crystals, which may have many symmetries, is relatively easy to appreciate. Other applications of groups to physics are more subtle, and we can only hint at their nature here. Simple symmetries have many applications; for example, the spherical symmetry of the sun leads to the fact that the orbits of planets are planar (to a good approximation). However, there are many areas of physics in which more complicated symmetries are considered.

One such area relates to the vibration of molecules. Briefly, the atoms which comprise a molecule are arranged, relative to each other in three-dimensional space, in a standard configuration which is fairly rigid, but not entirely so. Indeed the atoms are able to make small vibrations about what is called their *equilibrium position*, rather as if they were connected together by coiled springs (see Figure 4.6(a)). The nature of these vibrations has implications for the frequency(s), and so colour(s) of

light which the molecule may emit or absorb. Thus an understanding of the possible vibrations in a given molecule is of importance.

To gain information about these vibrations, physicists consider the total energy of the molecule, which can be expressed as a formula involving the masses of the atoms, and their coordinates and velocities. By making a cunning change of coordinates in the underlying three-dimensional space, this formula can be greatly simplified, enabling the total energy to be expressed as a sum of energies corresponding to a finite number of basic periodic vibrations, known as *normal modes*. In this way, any vibration of the molecule can be thought of as a combination of normal modes.

It turns out that the symmetry group of the molecule can be used to obtain information about these normal modes. The method involves representing each of the elements of the symmetry group in an appropriate matrix form, and then applying a certain algorithm (a generalisation of diagonalisation) to reduce these matrices to a fundamental form, called *irreducible*.

Diagonalisation of 2×2 matrices was discussed in Chapter B3, Section 3.

The symmetry group of the water molecule is isomorphic to $(S(\square), \circ)$.
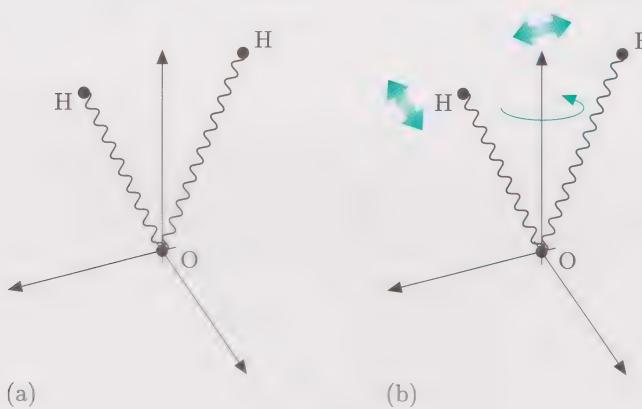
Figure 4.6   (a) The equilibrium position of a water molecule H_2O (b) Symmetries of this molecule

The above discussion is based on the classical model of atoms as point masses. Quantum mechanics, on the other hand, models all particles as wave functions which, roughly speaking, give the probability of observing the particle in any part of space. This theory was pioneered in the mid 1920s by W. Heisenberg and others, and it completely transformed our understanding of subatomic particles and their relationship with light. Because the symmetry properties of quantum mechanical systems entirely determine many of their other properties, quantum mechanics now makes fundamental use of groups. This was first recognised by E. P. Wigner in 1926 when he succeeded in deriving the wave function for a system of n identical particles. Quantum mechanics treats subatomic particles of the same type as being indistinguishable, and so such a system is invariant under permutations, or rearrangements, of the particles. The set of permutations of any n objects forms a group under the operation of composition, called the **symmetric group S_n**, and Wigner was able to solve the n particle problem by drawing on what he referred to as

The order of the group S_n is $n! = n \times (n-1) \times \ldots \times 1$.

> 'a well-developed mathematical theory ... of transformation groups which are isomorphic with the symmetric group'.

From that moment, it was clear that to understand the physical world at its deepest level physicists would have to learn some group theory!

4.3 Unexpected groups

Amongst the most remarkable of all groups are those associated with the so-called **elliptic curves**, which have equations of the form

$$y^2 = ax^3 + bx^2 + cx + d, \text{ where } a \neq 0.$$

All such elliptic curves are symmetric under reflection in the x-axis, because of the term y^2 on the left-hand side. Figure 4.7 shows an example of an elliptic curve, $y^2 = x^3 - 2x$. Note that points on this curve include: $(-1, -1)$, $(-1, 1)$, $(0, 0)$, $(2, 2)$ and $(2, -2)$.

We now describe how to associate a group with such a curve. Let G denote the set of points on the curve, together with an extra point, called e, which is to be thought of as lying 'at infinity'. Next, we define a binary operation $*$ on the set G as follows. Given points p and q in G, we draw the straight line l through p and q, find the other point where l meets the curve, and then take $p * q$ to be the reflection of this other point in the x-axis.

Figure 4.7 illustrates this process. We see that the line joining $(-1, -1)$ to $(0, 0)$, which is $y = x$, meets the curve again at $(2, 2)$. The reflection of this point in the x-axis is $(2, -2)$, so

$$(-1, -1) * (0, 0) = (2, -2).$$
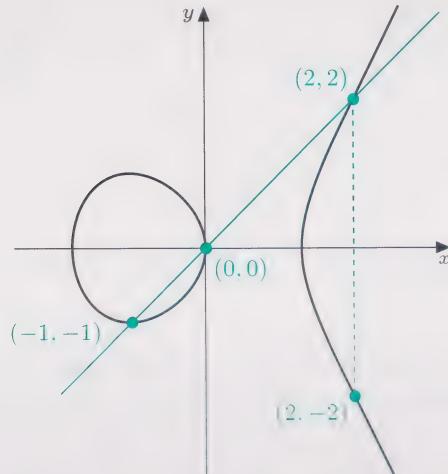
Figure 4.7 The elliptic curve $y^2 = x^3 - 2x$, and the construction to find $(-1, -1) * (0, 0)$

Several cases of this definition need to be dealt with separately. For example, if $p = e$ or $q = e$, then the line l is taken to be vertical, so

$$p * e = p = e * p.$$

Thus e forms an identity. If $p = q \neq e$, then l is taken to be the tangent line to the elliptic curve at p. Though this is not obvious, the only situation where the line joining points p and q does not meet the curve again is when this line is vertical. In this situation, we take $p * q$ to be e (so the inverse of the point $p = (x, y)$ is $q = (x, -y)$).

Once such details have been taken care of, it can be shown that $(G, *)$ forms an infinite Abelian group, with identity e. The hardest axiom to verify is G4, associativity. Although this involves only algebraic methods that you have met, it is difficult, and you are not recommended to try it!

The most remarkable thing about such groups is not their weird construction, but their extraordinary range of applications. Suffice it to say that:

◇ such groups based on elliptic curves played a key role in the proof of Fermat's Last Theorem;

◇ the construction can be adapted to generate a huge supply of *finite* Abelian groups and these can be exploited to produce public key ciphers which are potentially harder to break than RSA ciphers;

◇ the groups associated with elliptic curves form the basis of one of the most powerful techniques known for factorising larger integers, so they are relevant to the process of breaking RSA ciphers!

4.4 Group theory – the beginning, and the end?

Perhaps the best-known formula in mathematics is the one giving the solutions to the general quadratic equation $ax^2 + bx + c = 0$, with $a \neq 0$:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This formula was known in essence to the Ancient Babylonians.

There are similar, but more complicated, formulas for solving the general cubic equation and the general quartic equation. These formulas, found in the sixteenth century, involve the usual arithmetic operations $+, -, \times, \div$, together with nth roots, applied to the coefficients of the equation. A formula has never been found, however, for solving a general quintic equation, and in the nineteenth century N. H. Abel (1826) and E. Galois (1831) proved that no such formula exists. They used methods, introduced by J. L. Lagrange in 1771, which form the very beginnings of group theory.

The idea of the proof is to associate with each polynomial equation a finite group, called the **Galois group** of the equation. One then shows that if the equation *can* be solved by a formula, then the corresponding Galois group must have a certain very special property, which does *not* hold for the Galois group of a general quintic equation.

The elements of the Galois group of a polynomial equation are those permutations of the roots of the equation which, roughly speaking, leave invariant the algebraic relations satisfied by the roots. It turns out that a polynomial equation has a formula for its roots if and only if its Galois group G has a sequence of subgroups $\{e\} = G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$ with certain special properties.

Now the Galois group of a *general* quintic equation has $5! = 120$ elements; each of the possible permutations of the five roots has no effect on the algebraic relations amongst the roots. A group with 120 elements may seem rather large, but it is a routine matter to check that it has no such special sequence of subgroups. Therefore, there is no formula giving the solutions of a general quintic equation.

As this result became more widely known and understood towards the end of the nineteenth century, the related concept of a **simple group** assumed importance. Roughly speaking, finite simple groups are related to finite groups in the way that prime numbers are related to positive integers; they form the basic building blocks. The 'simplest' finite simple groups are the cyclic groups of order p, where p is a prime number, but there are several other infinite families of simple groups.

The work of Evariste Galois went deeper than Abel's, and he was the first to use the word 'group'. But Galois was unable to make his methods comprehensible to mathematicians of his day, and he died in 1832, aged 20, in a duel.

A more complete, though non-technical, account of Galois groups, as well as other applications of groups, can be found in I. N. Stewart, *From here to Infinity*, Oxford University Press, 1996.

A key role in this classification is played by the result that every finite group of *even* order contains a self-inverse element different from e; this follows from Lemma 3.1.

The classification of *all* finite simple groups was finally completed in 1983. It involves contributions by many group theorists and covers some thousands of printed pages. The result is that every finite simple group belongs to one of the several known infinite families or to a set of 26 oddities, the so-called **sporadic groups**. The largest of these sporadic groups, known as the Monster, has

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$$

elements. It is a group of rotations in $196\,883$–dimensional space!

The completion of this extraordinary classification does not mean the end of research in group theory; many unanswered questions about finite simple groups remain. More importantly, however, any attempt to solve a problem by making use of some underlying symmetry will lead to groups; and the more intricate that symmetry is, the more deeply we need to delve into group theory to help solve the problem.

Summary of Chapter D3

A set with a binary operation on it satisfying specified properties form a group. The axioms for a group (closure, identity, inverses and associativity) were given in Section 2. You met various specific groups, including the following.

$(S(X), \circ)$	Symmetries of a plane set X under composition
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ under $+$	Various sets of numbers under addition
$\mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ under $\times$	Various sets of non-zero numbers under multiplication
$(\mathbb{Z}_n, +_n)$	$\mathbb{Z}_n$ under modular addition
$(\mathbb{Z}_p^*, \times_p)$	$\mathbb{Z}_p^*$ under modular multiplication (p must be prime)

Two finite groups $(G, *)$ and $(H, \diamond)$ are isomorphic to each other if there is a one-one function from G onto H that converts a Cayley table for $(G, *)$ into one for $(H, \diamond)$. Isomorphic groups share their properties *as groups*, such as the number of self-inverse elements and whether or not they are Abelian.

You saw that all groups of order 1 are isomorphic, as are all groups of order 2 and of order 3. There are essentially two different groups of order 4: $(\mathbb{Z}_4, +_4)$ and $(S(\square), \circ)$. We asserted that all groups of order up to 8 are isomorphic to one of the groups listed in the table in the summary of Section 3 and repeated below.

Group	Order	Self-inverses	Abelian
$(\{e\}, *)$	1	1	✓
$(\mathbb{Z}_2, +_2)$	2	2	✓
$(\mathbb{Z}_3, +_3)$	3	1	✓
$(\mathbb{Z}_4, +_4)$	4	2	✓
$(S(\square), \circ)$	4	4	✓
$(\mathbb{Z}_5, +_5)$	5	1	✓
$(\mathbb{Z}_6, +_6)$	6	2	✓
$(S(\triangle), \circ)$	6	4	✗
$(\mathbb{Z}_7, +_7)$	7	1	✓
$(\mathbb{Z}_8, +_8)$	8	2	✓
$(S(\square), \circ)$	8	6	✗
$(S(\text{BOX}), \circ)$	8	8	✓
$(S(\text{ROTOR}), \circ)$	8	4	✓
$(QUAT, \times)$	8	2	✗

Learning outcomes

You have been working towards the following learning outcomes.

Notation to know and use

r_θ, q_ϕ, $S(X)$, $S(\triangle)$, $S(\square)$, $S(\square)$, $(S(X), \circ)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_p^*, \times_p)$.

Terms to know and use

Isometry (in $\mathbb{R}^2$); symmetry (of a plane set); identity transformation; group; subgroup; self-inverse (element of a group); order of a group; finite group; infinite group; Abelian group; isomorphism.

Mathematical skills

Each skill applies only in suitable cases.

◇   Recognise the symmetries of a given plane set, in particular translations, rotations and reflections.

◇   Calculate the result of composing isometries of the form r_θ and q_ϕ using Table 1.3.

◇   For a bounded plane set, centred at the origin, find all its symmetries. Show in a Cayley table how the symmetries of such a plane set combine under composition.

◇   Calculate a Cayley table for a finite set with a specified operation (such as a set of integers with modular addition, or a set of 2×2 matrices with matrix multiplication).

◇   Check whether a particular finite set and operation form a group by examination of a Cayley table (possibly using prior knowledge that the operation is associative).

◇   Check whether a particular set and operation form a group by checking the group axioms.

◇   Follow manipulations involving members of an unspecified group.

◇   Determine whether a particular group is Abelian, either by examining a Cayley table (for a finite group), or otherwise.

◇   Show that particular finite groups are isomorphic to each other by examining their Cayley tables (possibly after a suitable reordering of the elements).

◇   Show that particular finite groups are not isomorphic to each other, by noting differences in their properties.

◇   Classify a group of order up to 8 by matching its properties to those in the table in the summary of Section 3.

Solutions to Activities

Solution 1.1

(a) (i) There are three possible places to which ○ may move (each of the three 'propeller blades'). For each of these, ● can move to two places. So we expect set A to have $3 \times 2 = 6$ symmetries.

(ii) Set A has an identity symmetry (rotation through 0), and two non-trivial rotational symmetries, through $2\pi/3$ and $4\pi/3$ (see Figure S.1(b) and (c)). It also has three reflectional symmetries, shown in Figure S.1(d)-(f). That does give a total of six symmetries, as expected.
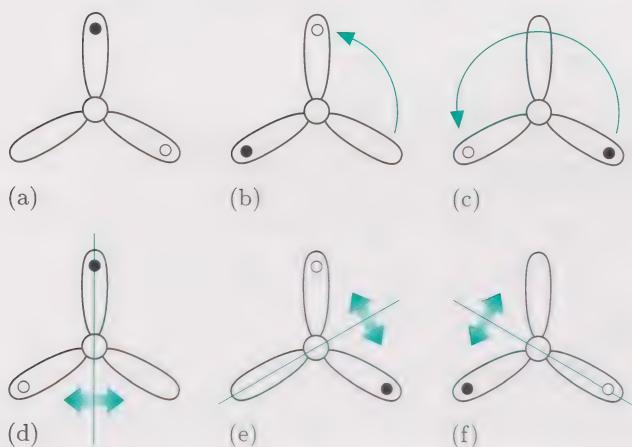
Figure S.1 Symmetries of the set A from Figure 1.1(a)

(b) Set B has four rotational symmetries: through angles 0, $\pi/2$, π, and $3\pi/2$. It has no reflectional symmetries. The three non-trivial symmetries are shown on a single diagram in Figure S.2.
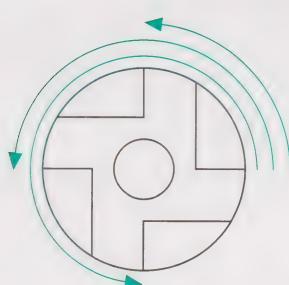
Figure S.2 Symmetries of the set B from Figure 1.1(b)

(c) The snowflake has six rotational symmetries (through angles 0, $\pi/3$, $2\pi/3$, π, $4\pi/3$, $5\pi/3$) and six reflectional symmetries (in axes through its centre, the angle between adjacent axes being $\pi/6$), making twelve in all. The non-trivial symmetries are shown in Figure S.3.
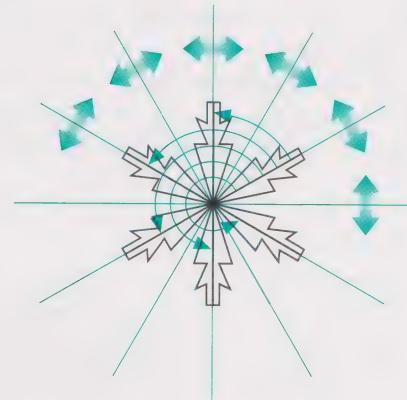
Figure S.3 Symmetries of the set C from Figure 1.1(c)

Solution 1.3

(a) Here $r_{\pi/2}$ is rotation through $\pi/2$, and
$$r_{\pi/2}(1,1) = (-1,1).$$

(b) Here $q_{\pi/2}$ is reflection in the y-axis, and
$$q_{\pi/2}(1,1) = (-1,1).$$

(c) Here $q_{\pi/4}$ is reflection in the line $y = x$, and
$$q_{\pi/4}(2,0) = (0,2).$$

(d) Here $r_{\pi/4}$ is rotation through $\pi/4$, and
$$r_{\pi/4}(1,0) = (1/\sqrt{2}, 1/\sqrt{2}).$$

Solution 1.4

Refer to Figure S.1 for $S(A)$, to Figure S.2 for $S(B)$ and to Figure S.3 for $S(C)$. We find that:

$S(A) = \{e, r_{2\pi/3}, r_{4\pi/3}, q_{\pi/6}, q_{\pi/2}, q_{5\pi/6}\};$
$S(B) = \{e, r_{\pi/2}, r_\pi, r_{3\pi/2}\};$
$S(C) = \{e, r_{\pi/3}, r_{2\pi/3}, r_\pi, r_{4\pi/3}, r_{5\pi/3}, q_0, q_{\pi/6}, q_{\pi/3},$
$\qquad q_{\pi/2}, q_{2\pi/3}, q_{5\pi/6}\}.$

Solution 1.6

(a) If we first rotate through an angle π, and then rotate through an angle $\pi/2$, the result of the combined transformation is a rotation through a total angle of $\pi + \pi/2 = 3\pi/2$. So

$$r_{\pi/2} \circ r_\pi = r_{3\pi/2}.$$

(b) If we reflect in the same line twice in succession, then we return to where we started, whatever the axis of reflection may be. So

$$q_{\pi/4} \circ q_{\pi/4} = e.$$

(c) The effect of this composite symmetry on a marked disc is shown in Figure S.4 (where (a) shows the initial position and (b) the position after: first q_0, then $r_{\pi/2}$), and we see from the figure that it is the same as the reflection $q_{\pi/4}$. So

$$r_{\pi/2} \circ q_0 = q_{\pi/4}.$$

(a)   (b)
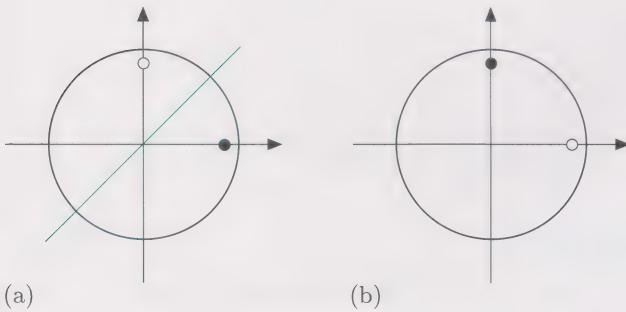
Figure S.4

(d) The effect of this composite symmetry on a marked disc is shown in Figure S.5 (where (a) shows the initial position and (b) the position after: first $q_{3\pi/4}$, then $q_{\pi/4}$), and we see from the figure that it is the same as that of rotation through an angle π. So

$$q_{\pi/4} \circ q_{3\pi/4} = r_\pi.$$

(a)   (b)
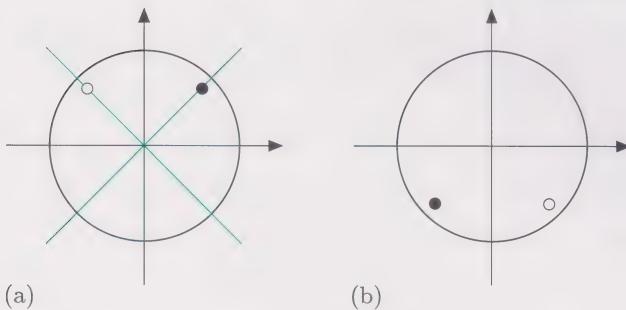
Figure S.5

Solution 1.8

We obtain the following Cayley table.

$\circ$	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$
e	e	$r_{\pi/2}$	r_π	$r_{3\pi/2}$
$r_{\pi/2}$	$r_{\pi/2}$	r_π	$r_{3\pi/2}$	e
r_π	r_π	$r_{3\pi/2}$	e	$r_{\pi/2}$
$r_{3\pi/2}$	$r_{3\pi/2}$	e	$r_{\pi/2}$	r_π

Solution 2.1

The inverses are as follows.

symmetry	e	$r_{2\pi/3}$	$r_{4\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$
inverse	e	$r_{4\pi/3}$	$r_{2\pi/3}$	$q_{\pi/6}$	$q_{\pi/2}$	$q_{5\pi/6}$

Clearly e and the three reflections are self-inverse, as specified by (a) and (c) in Theorem 2.1. Also, both $r_{2\pi/3}$ and $r_{4\pi/3}$ satisfy Theorem 2.1(b). We have

$$r_{2\pi/3}^{-1} = r_{2\pi - 2\pi/3} = r_{4\pi/3};$$
$$r_{4\pi/3}^{-1} = r_{2\pi - 4\pi/3} = r_{2\pi/3}.$$

Solution 2.2

Using the Cayley table, we obtain

$$r_{\pi/2} \circ (q_{\pi/4} \circ r_{3\pi/2}) = r_{\pi/2} \circ q_{\pi/2} = q_{3\pi/4}$$

and

$$(r_{\pi/2} \circ q_{\pi/4}) \circ r_{3\pi/2} = q_{\pi/2} \circ r_{3\pi/2} = q_{3\pi/4},$$

so the associative property holds in this particular case.

Solution 2.3

You need to check the four group axioms G1–G4.

Closure   Suppose that a and b are in $\mathbb{R}^*$, so a and b are both non-zero real numbers. Then $a \times b$ is certainly a real number, and cannot be zero (since $a \times b = 0$ only if $a = 0$ or $b = 0$).

Identity   The number 1 is in $\mathbb{R}^*$, and, for all a in $\mathbb{R}^*$, we have

$$a \times 1 = a = 1 \times a.$$

So 1 is an identity element for $\mathbb{R}^*$.

Inverses   For any a in $\mathbb{R}^*$, we have $a \neq 0$, so $1/a$ is defined, and is in $\mathbb{R}^*$. We have

$$a \times (1/a) = 1 = (1/a) \times a,$$

so $1/a$ is an inverse for a in $(\mathbb{R}^*, \times)$.

Associativity   Since $\times$ is associative on $\mathbb{R}$, it must be associative on $\mathbb{R}^*$, since $\mathbb{R}^*$ is a subset of $\mathbb{R}$.

Hence $(\mathbb{R}^*, \times)$ satisfies the group axioms, and so forms a group.

Solution 2.4

A Cayley table for $(\{1, -1\}, \times)$ is given below.

$\times$	1	-1
1	1	-1
-1	-1	1

All the entries in the table lie in $\{1, -1\}$, and so multiplication is closed on this set (Axiom G1).

Since the operation is multiplication of numbers, 1 forms an identity element (Axiom G2).

We have

$$1 \times 1 = 1 \quad \text{and} \quad (-1) \times (-1) = 1,$$

so each element of $\{1, -1\}$ has a multiplicative inverse in the set (Axiom G3).

Since multiplication is associative on $\mathbb{R}$, it is also associative on $\{1, -1\}$ (Axiom G4).

Thus $(\{1, -1\}, \times)$ is a group.

Also the Cayley table is symmetric about the main diagonal, so this group is Abelian.

Solution 2.5

(a) The Cayley table is

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Each entry in the body of the table is in the set $\{1, 3, 5, 7\}$, so G1 holds.

The row and column corresponding to 1 repeat the borders of the table, so 1 is an identity, and G2 holds.

The identity element 1 appears in each row and column, and these appearances are symmetric, so G3 holds.

Finally, $\times_8$ is associative on $\mathbb{Z}_8^*$, and so on its subset $\{1, 3, 5, 7\}$, so G4 holds. Hence $(\{1, 3, 5, 7\}, \times_8)$ is a group.

(b) The Cayley table is

$+_{10}$	2	4	6	8
2	4	6	8	0
4	6	8	0	2
6	8	0	2	4
8	0	2	4	6

Here, 0 appears in the body of the table, but 0 is *not* in the set $\{2, 4, 6, 8\}$. Hence axiom G1 fails, so this is not a group. (Also, there is no identity element, so G2 fails.)

(c) The Cayley table is

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

Each entry in the body of the table is in the set $\{2, 4, 6, 8\}$, so G1 holds.

Here, the row and column corresponding to the element 6 repeat the borders of the table, so 6 is an identity, and G2 holds.

The identity element 6 appears in each row and column, and these appearances are symmetric, so G3 holds.

Finally, $\times_{10}$ is associative on $\mathbb{Z}_{10}^*$, and so on its subset $\{2, 4, 6, 8\}$, so G4 holds. We deduce that $(\{2, 4, 6, 8\}, \times_{10})$ is a group, with identity 6.

Solution 2.6

(a) The Cayley table is

$\times$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{I}$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$
$\mathbf{A}$	$\mathbf{A}$	$\mathbf{B}$	$\mathbf{C}$	$\mathbf{I}$
$\mathbf{B}$	$\mathbf{B}$	$\mathbf{C}$	$\mathbf{I}$	$\mathbf{A}$
$\mathbf{C}$	$\mathbf{C}$	$\mathbf{I}$	$\mathbf{A}$	$\mathbf{B}$

All the entries in the table are in the set $M = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$, so G1 holds. The element $\mathbf{I}$ acts as identity, and it appears symmetrically in each row and column, so axioms G2 and G3 hold. Finally, matrix multiplication is associative, so G4 also holds. Hence $\{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}\}$ is a group under matrix multiplication.

(b) $\mathbf{I}$, $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ represent e, $r_{\pi/2}$, r_π and $r_{3\pi/2}$, respectively, and the set $\{e, r_{\pi/2}, r_\pi, r_{3\pi/2}\}$ is $S(\text{TRIM})$, the symmetries of the wheel trim in Figure 1.1(b), as found in Activity 1.4. So $(M, \times)$ corresponds to $(S(\text{TRIM}), \circ)$.

Solution 2.8

If h and h' are both inverses of g, then

$$h * g = e \quad \text{and} \quad g * h' = e.$$

Thus, using the suggestion,

$$(h * g) * h' = e * h' = h' \quad \text{(by G2)}$$

and

$$h * (g * h') = h * e = h \quad \text{(by G2)}.$$

Hence, by G4,

$$h' = (h * g) * h' = h * (g * h') = h.$$

Thus $h = h'$, so g has a unique inverse.

Solution 2.9

Considering: first row e; then column e; then column c; then row b, allows us to fill in four further entries.

*	e	a	b	c
e	e	a	b	c
a	a			b
b	b	c	a	e
c	c			a

Next, note that column a contains a and c, while row a contains b, so the only element left for the row a, column a entry is e. We can then use the 'once in each row and column' property to complete the table, as below.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Solution 3.1

(a) An isomorphism is provided by the function $\varphi : \mathbb{Z}_4 \longrightarrow S(\text{TRIM})$, where $\varphi(0) = e$, $\varphi(1) = r_{\pi/2}$, $\varphi(2) = r_\pi$, $\varphi(3) = r_{3\pi/2}$. Notice that this function maps the borders of the Cayley table for $(\mathbb{Z}_4, +_4)$, given in Table 3.1, into those of the Cayley table for $(S(\text{TRIM}), \circ)$. Furthermore, it maps each entry within the Cayley table of $(\mathbb{Z}_4, +_4)$ to the entry at the corresponding place in the Cayley table of $(S(\text{TRIM}), \circ)$. Hence φ is indeed an isomorphism between $(\mathbb{Z}_4, +_4)$ and $(S(\text{TRIM}), \circ)$.

(b) The Cayley table of $(\mathbb{Z}_3, +_3)$ is

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The upper left quarter of the Cayley table for $S(\triangle)$ is reproduced below. Notice that it shows the pattern of constant diagonals, shared by that for $(\mathbb{Z}_3, +_3)$.

$\circ$	e	$r_{2\pi/3}$	$r_{4\pi/3}$
e	e	$r_{2\pi/3}$	$r_{4\pi/3}$
$r_{2\pi/3}$	$r_{2\pi/3}$	$r_{4\pi/3}$	e
$r_{4\pi/3}$	$r_{4\pi/3}$	e	$r_{2\pi/3}$

Examination of this part of the Cayley table for $S(\triangle)$ shows that the set $\{e, r_{2\pi/3}, r_{4\pi/3}\}$ has the following properties.

> It is closed under composition.
> It contains the identity, e.
> It contains the inverse of each of its members.

So this set forms a subgroup of $(S(\triangle), \circ)$, and this subgroup is isomorphic to $(\mathbb{Z}_3, +_3)$. An isomorphism is provided by the function ψ, where $\psi(0) = e$, $\psi(1) = r_{2\pi/3}$, $\psi(2) = r_{4\pi/3}$.

Solution 3.2

(a) Cayley tables for $(\mathbb{Z}_2, +_2)$ and for $(\{e, r_\pi\}, \circ)$ are given below. The second table shows that $(\{e, r_\pi\}, \circ)$ forms a symmetry group that is isomorphic to $(\mathbb{Z}_2, +_2)$. (An isomorphism is provided by $\phi(0) = e$, $\phi(1) = r_\pi$.)

$+_2$	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, +_2)$

$\circ$	e	r_π
e	e	r_π
r_π	r_π	e

$(\{e, r_\pi\}, \circ)$

Any plane set with just one rotational symmetry and no reflectional symmetries will have this symmetry group. One example is shown in Figure S.6.
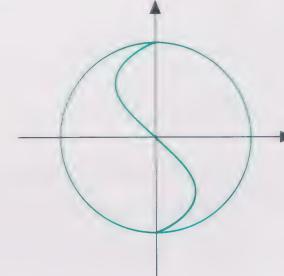
Figure S.6

(b) We noted in the solution to Activity 3.1(b) that $\{e, r_{2\pi/3}, r_{4\pi/3}\}$ forms a group of symmetries isomorphic to $(\mathbb{Z}_3, +_3)$. We saw there that this is a subgroup of $S(\triangle)$, which suggests that we modify an equilateral triangle to retain rotational symmetries but lose the reflectional symmetries, as in Figure 1.25(b). (There are many other plane sets with this same symmetry group.)

Solution 3.3

Since 6 is the identity of this group, we place it first. Next, to obtain the pattern 6, 4, 6, 4 on the main diagonal to match the Cayley table of $\mathbb{Z}_4$, we place 4 third. Finally, we put 2 and 8 in the remaining positions (either way round), giving the following tables.

$\times_{10}$	6	2	4	8
6	6	2	4	8
2	2	4	8	6
4	4	8	6	2
8	8	6	2	4

$\times_{10}$	6	8	4	2
6	6	8	4	2
8	8	4	2	6
4	4	2	6	8
2	2	6	8	4

In each case the tables have the 'constant diagonals' property, so the two functions ϕ and ψ from $\mathbb{Z}_4$ to $\{2, 4, 6, 8\}$, given by

$$\phi(0) = 6, \quad \phi(1) = 2, \quad \phi(2) = 4, \quad \phi(3) = 8,$$

and

$$\psi(0) = 6, \quad \psi(1) = 8, \quad \psi(2) = 4, \quad \psi(3) = 2,$$

are both isomorphisms.

Solution 3.4

The group $(\{1, 3, 5, 7\}, \times_8)$ in Activity 2.5(a) has Cayley table:

$\times_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

The pattern in this Cayley table is the same as the pattern in the Cayley table of $S(\square)$, an isomorphism being:

$$\phi(e) = 1, \quad \phi(r_\pi) = 3, \quad \phi(q_0) = 5, \quad \phi(q_{\pi/2}) = 7.$$

(In fact, there are five other isomorphisms between $S(\square)$ and $\{1, 3, 5, 7\}$, obtained by rearranging the Cayley table of $\{1, 3, 5, 7\}$ using the orders $\{1, 3, 7, 5\}$, $\{1, 5, 7, 3\}$, $\{1, 5, 3, 7\}$, $\{1, 7, 3, 5\}$ and $\{1, 7, 5, 3\}$.)

The group $(\{2, 4, 6, 8\}, \times_{10})$ has two self-inverse elements, while $(S(\square), \circ)$ has four, so these groups are not isomorphic to each other.

Solution 3.5

(a) The group $(\mathbb{Z}_6, +_6)$ has two self-inverse elements 0 and 3; see the table below.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

However, $(S(\triangle), \circ)$ has four self-inverse elements, $e, q_{\pi/6}, q_{\pi/2}$ and $q_{5\pi/6}$; see the Comment on Activity 1.7(c). Hence by Theorem 3.1(b), these two groups are not isomorphic to each other. (Alternatively, note that $(\mathbb{Z}_6, +_6)$ is Abelian but $(S(\triangle), \circ)$ is not Abelian, and use Theorem 3.1(c).)

(b) The approach used in Activity 3.2(b) suggests that the set required can be obtained by modifying a regular hexagon, in order to retain the rotational symmetries but lose the reflectional symmetries, as in the set A in Figure S.7.
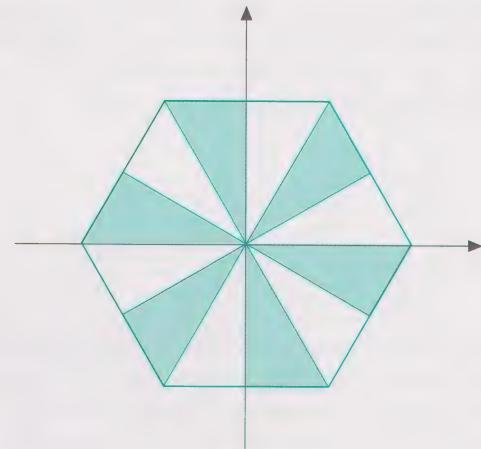

Figure S.7

The Cayley table of the symmetry group $(S(A), \circ)$ has the same constant diagonal pattern as that of $(\mathbb{Z}_6, +_6)$. See below.

$\circ$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$
e	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$
$r_{\pi/3}$	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e
$r_{2\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$
r_π	r_π	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$
$r_{4\pi/3}$	$r_{4\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π
$r_{5\pi/3}$	$r_{5\pi/3}$	e	$r_{\pi/3}$	$r_{2\pi/3}$	r_π	$r_{4\pi/3}$

The identical patterns in the Cayley tables indicate that the function:

$$\phi(0) = e, \quad \phi(1) = r_{\pi/3}, \quad \phi(2) = r_{2\pi/3},$$
$$\phi(3) = r_\pi, \quad \phi(4) = r_{4\pi/3}, \quad \phi(5) = r_{5\pi/3},$$

is an isomorphism. Hence $(\mathbb{Z}_6, +_6)$ and $(S(A), \circ)$ are isomorphic to each other.

55

Solution 3.6

(a) Any group $(G, *)$ of order 2 must be of the form
$\{e, a\}$. The 'once in each row and column'
property shows that the Cayley table must be:

$*$	e	a
e	e	a
a	a	e

Hence G is isomorphic to $(\mathbb{Z}_2, +_2)$, with
isomorphism ϕ given by:

$$\phi(0) = e, \quad \phi(1) = a.$$

(b) Any group $(G, *)$ of order 3 has three elements,
one of which is the identity (e say). Calling the
other two elements a and b, we have $G = \{e, a, b\}$
and the following partial Cayley table.

$*$	e	a	b
e	e	a	b
a	a		
b	b		

If the entry in row a, column a were e, then the
entry in row a column b would be b. But this is
not possible, since that would put two bs in
column b. Hence the entry in row a column a
must be b (since it is neither e nor a). Then the
'once in each row and column' property shows
that the Cayley table must be:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Hence G is isomorphic to $(\mathbb{Z}_3, +_3)$, with
isomorphism ϕ given by:

$$\phi(0) = e, \quad \phi(1) = a, \quad \phi(2) = b.$$

Solutions to Exercises

Solution 1.1

(a)
$$q_{\pi/4} \circ q_{\pi/2} = r_{2(\pi/4)-2(\pi/2) \ (\text{mod} \ 2\pi)}$$
$$= r_{-\pi/2 \ (\text{mod} \ 2\pi)}$$
$$= r_{3\pi/2}$$

(b)
$$q_{\pi/2} \circ q_{\pi/4} = r_{2(\pi/2)-2(\pi/4) \ (\text{mod} \ 2\pi)}$$
$$= r_{\pi/2}$$

(c)
$$r_{2\pi/3} \circ q_{\pi/4} = q_{7\pi/12}$$

(d)
$$q_{\pi/4} \circ r_{2\pi/3} = q_{-\pi/12 \ (\text{mod} \ \pi)} = q_{11\pi/12}$$

Solution 1.2

Set A has only one non-trivial symmetry, namely reflection in the y-axis, so $S(A) = \{e, q_{\pi/2}\}$.

$\circ$	e	$q_{\pi/2}$
e	e	$q_{\pi/2}$
$q_{\pi/2}$	$q_{\pi/2}$	e

Set B has only rotational symmetries: through 0 (the identity), $2\pi/3$ and $4\pi/3$, so $S(B) = \{e, r_{2\pi/3}, r_{4\pi/3}\}$.

$\circ$	e	$r_{2\pi/3}$	$r_{4\pi/3}$
e	e	$r_{2\pi/3}$	$r_{4\pi/3}$
$r_{2\pi/3}$	$r_{2\pi/3}$	$r_{4\pi/3}$	e
$r_{4\pi/3}$	$r_{4\pi/3}$	e	$r_{2\pi/3}$

Set C has one rotational symmetry, through π. It is also symmetric under reflection in either the x- or the y-axis, but has no other reflectional symmetries, so $S(C) = \{e, r_\pi, q_0, q_{\pi/2}\}$.

$\circ$	e	r_π	q_0	$q_{\pi/2}$
e	e	r_π	q_0	$q_{\pi/2}$
r_π	r_π	e	$q_{\pi/2}$	q_0
q_0	q_0	$q_{\pi/2}$	e	r_π
$q_{\pi/2}$	$q_{\pi/2}$	q_0	r_π	e

Solution 2.1

(a) Let $G = \{2n : n \in \mathbb{Z}\}$. Since G is infinite, we check the group axioms in turn.

Closure Consider any two elements of G, say $2m$ and $2n$. Then

$$2m + 2n = 2(m+n) \in G,$$

so G is closed under $+$.

Identity Since $0 = 2 \times 0$, we have $0 \in G$, and

$$2n + 0 = 2n = 0 + 2n,$$

for all $n \in \mathbb{Z}$, so 0 is an identity element.

Inverses Consider any element of G, say $2n$. Then $2(-n) = -2n$ is in G, and

$$2n + (-2n) = 0 = (-2n) + 2n,$$

so each element in G has an inverse.

Associativity This holds since $+$ is associative on $\mathbb{Z}$.

Hence $(G, +)$ forms a group.

(b) Let $G = \{1, 5, 7, 11\}$. Since G is finite, we form a Cayley table.

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

All the elements in the body of the table are in G, so axiom G1 holds. The element 1 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold. Also G4 holds, since $\times_{12}$ is associative on $\mathbb{Z}_{12}$ and so on G. Hence $(G, \times_{12})$ is a group.

(c) Let $G = \{1, -1, i, -i\}$. Since G is finite, we form a Cayley table.

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

All the elements in the body of the table are in G, so axiom G1 holds. The element 1 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold. Also, G4 holds since $\times$ is associative on $\mathbb{C}$ and so on G. Hence $(G, \times)$ is a group.

(d) Let G be this set of matrices. We know that matrix multiplication is associative. We will check that: G is closed under multiplication; G contains an identity, and G is closed under inverses.

Closure Consider the product of two members of G. We have

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix},$$

which is of the correct form to be in G.

Identity   Taking $a = 0$, we see that

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is in G, so G contains an identity under multiplication. (We know that this matrix satisfies $\mathbf{AI} = \mathbf{A} = \mathbf{IA}$ for *any* matrix $\mathbf{A}$, and so this certainly holds for any matrix in G.)

Inverses   Using the formula for the inverse of a 2×2 matrix, we see that

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix},$$

which is of the correct form to be in G. Hence G contains an inverse of each of its elements. (We know for *any* non-singular matrix $\mathbf{A}$ that

$$\mathbf{AA}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A},$$

so $\mathbf{A}^{-1}$ is an inverse for $\mathbf{A}$ under matrix multiplication.)

Thus $(G, \times)$ is a group (and indeed, is a subgroup of the group of all non-singular matrices under multiplication).

(e) Let $G = \{1, 2, 4, 5, 7, 8\}$. Since G is finite, we form a Cayley table.

$\times_9$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

All the elements in the body of the table are in G, so axiom G1 holds. The element 1 is an identity, and appears symmetrically in each row and column, so axioms G2 and G3 hold. Also G4 holds, since $\times_9$ is associative on $\mathbb{Z}_9$ and so on G. Hence $(G, \times_9)$ is a group.

(f) Let $G = \{3, 6, 9, 12\}$. Since G is finite, we form a Cayley table.

$\times_{15}$	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

All the elements in the body of the table are in G, so axiom G1 holds. The element 6 is an identity and appears symmetrically in each row and column, so axioms G2 and G3 hold. Also G4 holds, since $\times_{15}$ is associative on $\mathbb{Z}_{15}$ and so on G. Hence $(G, \times_{15})$ is a group.

Solution 2.2

(a) We know that if $g \in G$, then g^{-1} satisfies

$$g * g^{-1} = e = g^{-1} * g.$$

The inverse of g^{-1} is the (unique) element k of G which satisfies

$$g^{-1} * k = e = k * g^{-1}.$$

Evidently $k = g$ satisfies these two equations, so g is the inverse of g^{-1}.

(b) The inverse of $g * h$ is the (unique) element k of G which satisfies

$$(g * h) * k = e = k * (g * h).$$

Now $k = h^{-1} * g^{-1}$ satisfies these two equations, because

$$\begin{aligned}
(g * h) &* (h^{-1} * g^{-1}) \\
&= g * (h * h^{-1}) * g^{-1} \text{ (by associativity)} \\
&= g * g^{-1} \text{ (since } h * h^{-1} = e) \\
&= e \text{ (since } g * g^{-1} = e),
\end{aligned}$$

and similarly

$$\begin{aligned}
(h^{-1} * g^{-1}) * (g * h) &= h^{-1} * (g^{-1} * g) * h \\
&= h^{-1} * h \\
&= e.
\end{aligned}$$

(c) If g, h and $g * h$ are all self-inverse, then

$$g^{-1} = g, \quad h^{-1} = h \quad \text{and} \quad (g * h)^{-1} = g * h.$$

By part (b), $(g * h)^{-1} = h^{-1} * g^{-1}$, so

$$g * h = h^{-1} * g^{-1} = h * g,$$

as required.

Solution 3.1

(a) The row and column for e reproduce the order of the elements on the borders, so e is the identity element.

Since every element on the main diagonal is the identity element, e, this group has 8 self-inverse elements. Matching this feature with those in the table in the summary of Section 3, we see that this group must be isomorphic to $(S(\text{BOX}), \circ)$.

(b) The groups in Exercise 2.1(a) and (d) are infinite and so are not isomorphic to any finite group.

The group $(G, \times_{12})$ in Exercise 2.1(b) has 4 elements, so it must be isomorphic to either $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$ in the summary table. Since G has 4 self-inverse elements, it must be isomorphic to $(S(\square), \circ)$. Comparing the Cayley tables, we see that one suitable isomorphism from $(G, \times_{12})$ to $(S(\square), \circ)$ is given by

$$\phi(1) = e, \quad \phi(5) = r_\pi, \quad \phi(7) = q_0, \quad \phi(11) = q_{\pi/2}.$$

(There are other possible isomorphisms here, as there are in the other cases below.)

The group $(G, \times)$ in Exercise 2.1(c) has 4 elements, so it must be isomorphic to either $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$ in the summary table. Since G has 2 self-inverse elements, it must be isomorphic to $(\mathbb{Z}_4, +_4)$. The Cayley table for G can be rearranged to give 'constant diagonals', as follows.

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

This shows that a suitable isomorphism ϕ from $(G, \times)$ to $(\mathbb{Z}_4, +_4)$ is given by

$$\phi(1) = 0 \quad \phi(i) = 1, \quad \phi(-1) = 2, \quad \phi(-i) = 3.$$

The group $(G, \times_9)$ in Exercise 2.1(e) has 6 elements, so it must be isomorphic to either $(\mathbb{Z}_6, +_6)$ or $(S(\triangle), \circ)$ in the summary table. Since G has 2 self-inverse elements, it must be isomorphic to $(\mathbb{Z}_6, +_6)$. The Cayley table for G can be rearranged to give 'constant diagonals', as follows.

$\times_9$	1	2	4	8	7	5
1	1	2	4	8	7	5
2	2	4	8	7	5	1
4	4	8	7	5	1	2
8	8	7	5	1	2	4
7	7	5	1	2	4	8
5	5	1	2	4	8	7

This shows that a suitable isomorphism ϕ from $(G, \times_9)$ to $(\mathbb{Z}_6, +_6)$ is given by

$$\phi(1) = 0, \quad \phi(2) = 1, \quad \phi(4) = 2, \quad \phi(8) = 3,$$
$$\phi(7) = 4, \quad \phi(5) = 5.$$

The group $(G, \times_{15})$ in Exercise 2.1(f) has 4 elements, so it must be isomorphic to either $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$ in the summary table. Since G has 2 self-inverse elements, it must be isomorphic to $(\mathbb{Z}_4, +_4)$. The Cayley table for G can be rearranged to give 'constant diagonals', as follows.

$\times_{15}$	6	3	9	12
6	6	3	9	12
3	3	9	12	6
9	9	12	6	3
12	12	6	3	9

This shows that a suitable isomorphism ϕ from $(G, \times_{15})$ to $(\mathbb{Z}_4, +_4)$ is given by

$$\phi(6) = 0, \quad \phi(3) = 1, \quad \phi(9) = 2, \quad \phi(12) = 3.$$

Solution 3.2

The group $(\mathbb{Z}_{10}, +_{10})$ has just 2 self-inverse elements, 0 and 5, whereas $(S(\text{PENT}), \circ)$ has 6 self-inverse elements

$$e, \ q_{\pi/10}, \ q_{3\pi/10}, \ q_{\pi/2}, \ q_{7\pi/10}, \ q_{9\pi/10}.$$

Thus $(\mathbb{Z}_{10}, +_{10})$ is not isomorphic to $(S(\text{PENT}), \circ)$, by Theorem 3.1(b).

Alternatively: We could use Theorem 3.1(c), since $(\mathbb{Z}_{10}, +_{10})$ is Abelian, by Theorem 2.3, but $(S(\text{PENT}), \circ)$ is non-Abelian; for example, $r_{2\pi/5} \circ q_{\pi/2} = q_{7\pi/10}$ whereas $q_{\pi/2} \circ r_{2\pi/5} = q_{3\pi/10}$, using Table 1.3.

Index